CCEVS Interpretations of the Common Criteria

(as of 06 April 2001)

These pages contain the collected interpretations that have been approved by the management of the Common Criteria Evaluation and Validation Scheme. (For more information on the CCEVS, and the applcability of these interpretations, please see the CCEVS home page).

Contents

Index of Approved Interpretations

The following is a list of interpretations that have been approved by CCEVS management, including those that have been superseded or rescinded. They are listed in numerical order, each followed by the date it was approved and, if applicable, superseded or rescinded.

- **I-0338: Configuration Items In The Absence Of Explicit Scope (2000-03-27)**
- **I-0339: Assurance Of RVM Is By Testing And Design Analysis (2000-03-27)**
- **I-0348: Audit Data Loss Prevention Method May Be Site-Selectable (2000-03-27)**
- **I-0351: User Attributes To Be Bound Should Be Specified (2000-03-27)**
- **I-0352: Rules Governing Binding Should Be Specifiable (2000-12-20)**

- **I-0353: Association Of Access Control Attributes With Subjects And Objects (Approved 2000-03-27; Superseded 2000-12-05)**
- **I-0354: Association Of Information Flow Attributes W/Subjects And Information (Approved 2000-03-27; Superseded 2000-12-11)**
- **I-0355: Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3 (Approved 2000-03-27; Superseded 2000-12-05)**
- **I-0362: Scope Of Permitted Refinements (2000-03-27)**
- **I-0363: Attribute Inheritance/Modification Rules Need To Be Included In Policy (2000-03-27)**
- **I-0364: Application Notes In Protection Profiles Are Informative Only (2000-03-27)**
- **I-0370: Clarification Of "Audit Records" (Approved 2000-03-27; Superseded 2000-12-05)**
- **I-0371: Some Modifications To The Audit Trail Are Authorized (Approved 2000-03-27; Superseded 2000-12-11)**
- **I-0373: FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical (Approved 2000-03-27; Superseded 2000-12-05)**
- **I-0375: Elements Requiring Authentication Mechanism (2001-03-15)**
- **I-0377: Settable Failure Limits Are Permitted (Approved 2000-03-27; Superseded 2000-12-05)**
- **I-0383: Content Of PP Claims Rationale (Approved 2000-03-27; Superseded 2000-12-05)**
- **I-0385: Identification Of Standards (2000-03-27)**
- **I-0389: Recovery To A Known State (2001-03-15)**
- **I-0393: A Completely Evaluated ST Is Not Required When TOE Evaluation Starts (2001-03-15)**
- **I-0394: Iteration Must Cover All Scopes (2000-12-20)**
- **I-0395: Security Attributes Include Attributes Of Information And Resources (2001-03-15)**
- **I-0397: Iteration On Assurance Components/Elements (2001-03-15)**
- **I-0405: American English Is An Acceptable Refinement (2000-12-20)**
- **I-0406: Automated Or Manual Recovery Is Acceptable (2001-03-15)**
- **I-0411: Guidance Includes AGD_ADM, AGD_USR, ADO, And ALC_FLR (2000-12-22)**
- **I-0416: Association Of Access Control Attributes With Subjects And Objects (2000-12-05)**
- **I-0417: Association Of Information Flow Attributes W/Subjects And Information (2000-12-11)**

- **I-0418: Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3 (2000-12-05)**
- **I-0422: Clarification Of "Audit Records" (2000-12-05)**
- **I-0423: Some Modifications To The Audit Trail Are Authorized (2000-12-11)**
- **I-0424: FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical (2000-12-05)**
- **I-0425: Settable Failure Limits Are Permitted (2000-12-05)**
- **I-0426: Content Of PP Claims Rationale (2000-12-05)**

Index of RIs sent from CCEVS to the CCIMB

The following queue entries have been sent as RIs to the CCIMB by CCEVS. They are listed in numerical order of queue entry number; each indicates the RI number (see http://www.commoncriteria.org for all RIs).

- **I-0378: Meaning Of Compliance Claims (maintained by the CCIMB as RI-112)**
- **I-0379: How To Require User/Admin Documentation For Functional Components (maintained by the CCIMB as RI-113)**
- **I-0382: TSF Architectural Protections Are Really Assurances (maintained by the CCIMB as RI-147)**

Mailing Lists

Public Interpretation Discussion Mailing List:
A mailing list, `cc-cmt` (Common Criteria NIAP Interpretations Comments), has been set up to provide a forum for public comment and discussion on proposed NIAP interpretations to the Common Criteria (CC) and the Common Evaluation Methodology (CEM). To subscribe, send an email to listproc@nist.gov. The body of the message should contain the line:

`subscribe cc-cmt` ***your-first-name your-last-name***

This will start a subscription for the "From:" address of the request Email. Archives of the `cc-cmt` list may be found at http://www.nist.gov/itl/div896/emaildir/cc-cmt/maillist.html

Public Interpretations Announcement Mailing List:
A companion list has been set up for mailings of approved interpretations. This list is `cc-in`. To subscribe, send an email to listproc@nist.gov. The body of the message should contain the line:

`subscribe cc-in` ***your-first-name your-last-name***

This will start a subscription for the "From:" address of the request Email. Archives of the `cc-in` list may be found at http://www.nist.gov/itl/div896/emaildir/cc-in/maillist.html

---

Questions on these pages, or comments on queue entries, should be addressed to: IWG@gibraltar.ncsc.mil .

I-0338: Configuration Items In The Absence Of Explicit Scope

NUMBER: I-0338
STATUS: Approved by TTAP/CCEVS Management
TYPE: NIAP Interpretation

TITLE: Configuration Items In The Absence Of Explicit Scope

EFFECTIVE DATE: 2000-03-27

SOURCE REFERENCE: CC v2.1 Part 3 Subclause 8.2 ACM_CAP.2
RELATED TO: <None>
CCIMB ENTRY: CCIMB-INTERP-0099

STATEMENT OF INTERPRETATION:

The following interprets the ACM_CAP.2 Component Developer Action Elements in contexts where no Configuration Management Scope (ACM_SCP Family) components are included in the PP/ST:

In environments where a protection profile or security target does not explicitly have a statement of the items to be under configuration management, the ACM_CAP.2.2D element does not apply.

SPECIFIC INTERPRETATION:

This problem could be corrected in the following fashion:

1. Delete ACM_CAP.2.2D.
2. Change ACM_CAP.2.3D to refer to a "configuration list" instead of "CM documentation".
3. Delete ACM_CAP.2.3C.
4. Change ACM_CAP.2.5C to refer to the "configuration list" instead of "CM documentation".
5. Change ACM_CAP.2.6C to refer to the "configuration list" instead of "the CM System".

Alternatively, ACM_CAP.2.D could be deleted, and ACM_CAP.2.6C could be changed to refer to "The CM documentation" instead of "The CM system".

If these changes are not made, an application note should be added to clarify the interpretation of ACM_CAP.2.2D when ACM_SCP is not included. The CEM should also be reviewed to determine any impact on the ACM_CAP work units for EAL2.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

The new contents elements introduced for the ACM_CAP.2 component all deal with uniquely identifying all items that make up the TOE and having their descriptions in a configuration list. This configuration list is contained in the CM documentation, which is required by ACM_CAP.2.3D. However, in the absence of explicit scope, there are no requirements that configuration management be performed on any of these items.

This viewpoint is supported by the Common Evaluation Methodology v1.0, which in the methodology for EAL2, ACM_CAP.2, does not impose any evaluator actions with respect to verifying use or presence of a CM system. In fact, the EAL2 work unit for ACM_CAP.2.6C (the only content and presentation element to refer to a CM system) requires a check only on the configuration list, not the CM system.

The requirements of the CEM lead to the conclusion that the goal of ACM_CAP in the absence of ACM_SCP is to ensure that an unambiguous list of all configuration items that comprise the TOE be maintained, but not that there necessarily be a full blown CM system in place to manage changes to those components.

I-0339: Assurance Of RVM Is By Testing And Design Analysis

NUMBER: I-0339
STATUS: Approved by TTAP/CCEVS Management
TYPE: NIAP Interpretation

TITLE: Assurance Of RVM Is By Testing And Design Analysis

EFFECTIVE DATE: 2000-03-27

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 10.10 FPT_RVM
CC v2.1 Part 2 Subclause J.10 FPT_RVM

RELATED TO:
I-0382 TSF Architectural Protections Are Really Assurances

CCIMB ENTRY: CCIMB-INTERP-0100

STATEMENT OF INTERPRETATION:

The following provides technical guidance regarding the element FPT_RVM.1.1: "The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed."

Assurance that FPT_RVM.1.1 is satisfied is achieved through a combination of testing and design analysis.

SPECIFIC INTERPRETATION:

To address this interpretation, the following should be added in the Part 2 Annex for FPT_RVM, at the end of the introductory paragraphs of Annex J.10:

> In order to provide assurance that this element is satisfied, the developer must provide a convincing argument that the design provides the enforcement, with this argument verified through testing. Foundations of such argument generally revolve around the construction of the interface to the TSF (e.g., call gates, network cards) and the limitations placed on those interfaces.

As this interpretation moves some of the verification burden from developer interface testing to the evaluator, as well as imposing additional requirements for developer arguments, changes to the CEM will be required.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

Most of the CC functional requirements are completely testable through the TSF interface. However, that is not true for this element. Determining the internal invocation sequence underlying a call is difficult to assure solely through testing. In such a case, examination of the design must come into play.

In order to provide assurance that this element is satisfied, the developer must provide a convincing argument that the design provides the enforcement, with this argument verified through testing. Foundations of such argument generally revolve around the construction of the interface to the TSF (e.g., call gates, network cards) and the limitations placed on those interfaces. In addition, the nature of the convincing argument should be based on the assurance package which has been chosen to be associated with the functional requirements. The depth (i.e., how much detail is involved) is dependent on the nature of assurance being pursued (i.e., the lower the level of assurance the less detail required).

The elements from Part 2 of the CC are usually testable through the TSF interface. This is not so for this element.

I-0348: Audit Data Loss Prevention Method May Be Site-Selectable

NUMBER: I-0348
STATUS: Approved by TTAP/CCEVS Management
TYPE: NIAP Interpretation

TITLE: Audit Data Loss Prevention Method May Be Site-Selectable

EFFECTIVE DATE: 2000-03-27

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 3.6 FAU_STG
CC v2.1 Part 2 Subclause C.6 FAU_STG
RELATED TO: <None>
CCIMB ENTRY: CCIMB-INTERP-0101

STATEMENT OF INTERPRETATION:

The following interprets the FAU_STG.4 component: "The TSF shall [selection: *'ignore auditable events', 'prevent auditable events, except those taken by the authorised user with special rights', 'overwrite the oldest stored audit records'*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full."

It is acceptable for the TSF to allow the actions to be taken when the audit trail is full to be site-configurable, as long as the TSF provides a pre-determined set of acceptable operations and an acceptable operation is defined as a default.

SPECIFIC INTERPRETATION:

To address this interpretation, the following new component should be added to the FAU_STG family:

FAU_STG.x Site-Configurable Prevention of Audit Loss

Management: FAU_STG.x

The following actions could be considered for the management functions in FMT:

1. Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.

Audit: FAU_STG.x

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

1. Basic: Actions taken due to the audit storage failure.
2. Basic: Selection of an action to be taken when there is an audit storage failure.

Hierarchical to: FAU_STG.4

FAU_STG.x.1. The TSF shall provide the capability to [selection: *'ignore auditable events', 'prevent auditable events, except those taken by the authorised user with special rights', 'overwrite the oldest stored audit records'*] and [assignment: *other actions to be taken in case of audit storage failure*], if the audit trail is full.

FAU_STG.x.2. The TSF shall [selection: *'ignore auditable events', 'prevent auditable events, except those taken by the authorised user with special rights', 'overwrite the oldest stored audit records'*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full and no other action has been selected.

Dependencies:

- FAU_STG.1 Protected Audit Trail Storage
- FMT_MTD.1 Management of TSF Data

The following should be added to the Part 2 Annex for the new component:

User Application Notes:

This component specifies the behaviours that the TOE must be capable of taking when the audit trail is full. It also provides a default behaviour to take if no behaviour is explicitly selected.

Potential behaviours that could be selected include the ability to ignore audit records, or to freeze the TOE such that no auditable events can take place. If the latter is selected, the requirement states that the authorised user with specific rights can continue to generate auditable events (actions). This permits the administrator to reset the system. Consideration should be given to the choice of the action to be taken by the TSF in the case of audit storage exhaustion, as ignoring events, which provides better availability of the TOE, will also permit actions to be performed without being recorded and without the user being accountable.

Operations

Selection:

In FAU_STG.x.1, the PP/ST author should select whether the TSF shall provide the ability to ignore auditable actions, prevent auditable actions from happening, and/or overwrite the oldest audit records.

In FAU_STG.x.2, the PP/ST author should select whether the TSF shall ignore auditable actions, prevent auditable actions from happening, and/or overwrite the oldest audit records if no action has been selected.

Assignment:

In FAU_STG.x.1, the PP/ST author should specify other actions that should be taken in case of audit storage failure, such as informing the authorised user.

In FAU_STG.x.2, the PP/ST author should specify other actions that should be taken in case of audit storage failure when no action has been selected, such as informing the authorised user.

Additionally, the management section for the existing FAU_STG.4 should be re-written to indicate that there are no management activities forseen.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

The FAU_STG.4 element explicitly states the actions to be taken by the TSF when the audit log is full. This wording implicitly disallows the actions to be taken to be site-selectable. Further, making such actions site selectable would not be an acceptable refinement, as an ST meeting the refined version would not meet the unrefined version.

As a result, a new component is required that allows site-selectable actions. Having the ability to have actions site-selectable increases the flexibility of the TOE, and allows the TOE to adjust to changing security needs.

This new component provides a default action to be taken if no explicit action is selected.

As part of the preparation of this component, it was uncovered that the management section for FAU_STG.4 indicates that site-selectable options are permitted, even though that is an improper refinement, and it is not mentioned as a possibility by the application notes.

I-0351: User Attributes To Be Bound Should Be Specified

NUMBER: I-0351
STATUS: Approved by TTAP/CCEVS Management
TYPE: NIAP Interpretation

TITLE: User Attributes To Be Bound Should Be Specified

EFFECTIVE DATE: 2000-03-27

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 7.6 FIA_USB.1
CC v2.1 Part 2 Subclause G.6 FIA_USB.1
RELATED TO:
I-0353 Association Of Access Control Attributes With Subjects And Objects
I-0354 Association Of Information Flow Attributes W/Subjects And Information
CCIMB ENTRY: CCIMB-INTERP-0102

STATEMENT OF INTERPRETATION:

The following interprets the FIA_USB.1 component:

PP or ST authors must be able to explicitly specify the user security attributes to be bound to subjects created on behalf of a user; refinement of the phrase "appropriate" is too vague.

SPECIFIC INTERPRETATION:

In order to address this interpretation, the following changes should be made to FIA_USB.1.1: (additions marked thusly; deletions marked thusly):

FIA_USB.1.1: The TSF shall associate the appropriate following user security attributes with subjects acting on behalf of that user: [assignment: *list of user security attributes to be bound*].

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

At the time a PP/ST is developed, the PP/ST author knows the significant attributes of the FSPs of the TOE, and which of those attributes are to be derived from user-based information. Thus, it is possible for the PP/ST author to specify which user attributes are to be bound to subjects created on the user's behalf.

However, in CC v2.1, the words of the FIA_USB.1.1 element use the word "appropriate". In order to specify the specific attributes to be bound, the PP/ST author must refine the element, and the evaluator must determine if the specified attributes are indeed "appropriate"; further, the evaluator must determine if there are appropriate attributes not included in the refined element. This creates a risk of inconsistent evaluator interpretation.

The ideal approach is to replace the need for refinement with an explicit assignment. The assignment should be driven by the attributes that are needed to enforce the TSP. For example, an access control policy based on user identity would require the user identity information be bound to the subject.

This interpretation should be distinguished from I-0353/I-0354, which discuss the security attributes bound to subjects, for not all subject security attributes derive from user attributes.

I-0352: Rules Governing Binding Should Be Specifiable

NUMBER:	I-0352
STATUS:	Approved by TTAP/CCEVS Management and Posted
TYPE:	NIAP Interpretation
TITLE:	Rules Governing Binding Should Be Specifiable
APPROVAL POSTING:	[cc-in 00013]
EFFECTIVE DATE:	2000-12-20
SOURCE REFERENCE:	CC v2.1 Part 2 Subclause 7.6 FIA_USB CC v2.1 Part 2 Subclause G.6 FIA_USB
RELATED TO:	<None>
CCIMB ENTRY:	CCIMB-INTERP-0137

ISSUE:

The current FIA_USB component provides the ability to associate "appropriate" user security attributes with subjects. It provides no mechanism to specify any rules governing the association, and it requires that the attributes to be mapped be provided through refinement.

However, in many cases it must be possible to specify how user attributes are mapped into subject attributes. An example would be the requirement that the label assigned to a subject is within the clearance range of the user. This is not expressable under the existing components.

STATEMENT OF INTERPRETATION:

A new component is added to the FIA_USB family that provides the ability to specify the rules governing the binding of user attributes to subjects.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1, Part 2: (additions marked thusly; deletions marked thusly)

- The following component is added to FIA_USB:

  FIA_USB.NIAP-0352-1: Expanded user-subject binding

  Hierarchical To: FIA_USB.1

  FIA_USB.NIAP-0352-1.1: The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

  FIA_USB.NIAP-0352-1.2: The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *initial association rules*].

  FIA_USB.NIAP-0352-1.3: The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *changing of attributes rules*].

  Dependencies: FIA_ATD.1 User Attribute Definition
- In Clause 7, Figure 7.1 is modified to show a new component, FIA_USB.NIAP-0352-1, that is immediately hierarchical to the existing FIA_USB.1.
- In Subclause 7.6, "Component Levelling" is modified to show a new component, FIA_USB.NIAP-0352-1, that is immediately hierarchical to the existing FIA_USB.1.
- In Subclause 7.6, the following paragraph is added after paragraph 295:

  FIA_USB.NIAP-0352-1 Expanded user-subject binding requires the specification of any rules governing the association between user attributes and the subject attributes into which they are mapped.
- In Subclause 7.6, the following Management section is added after paragraph 296:

  Management: FIA_USB.NIAP-0352-1

  The following actions could be considered for the management functions in FMT:

  a) an authorised administrator can define default subject security attributes.

  b) an authorised administrator can change subject security attributes.
- In Subclause 7.6, the following Audit section is added after paragraph 297:

  Audit: FIA_USB.NIAP-0352-1

  The following actions could be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

  a) Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject).

  b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).

- In Clause G, Figure G.1 is modified to show a new component, FIA_USB.NIAP-0352-1, that is immediately hierarchical to the existing FIA_USB.1.
- In Subclause G.6, the following is added after paragraph 1006:

  FIA_USB.NIAP-0352-1 Expanded user-subject binding

  User application notes

  The phrase "acting on behalf of" has proven to be a contentious issue in source criteria. It is intended that a subject is acting on behalf of the user who caused the subject to come into being or to be activated to perform a certain task. Therefore, when a subject is created, that subject is acting on behalf of the user who initiated the creation. In case anonymity is used, the subject is still acting on behalf of a user, but the identity of the user is unknown. A special category are the subjects that serve multiple users (e.g. a server process). In such cases the user that created this subject is assumed to be the "owner".

  Operations

  Assignment:

  In FIA_USB.NIAP-0352-1.1, the PP/ST author should specify a list of the user security attributes that are to be bound to subjects.

  Assignment:

  In FIA_USB.NIAP-0352-1.2, the PP/ST author should specify any rules that are to apply upon initial association of attributes with subjects, or "none".

  Assignment:

  In FIA_USB.NIAP-0352-1.3, the PP/ST author should specify any rules that are to apply when changes are made to the user security attributes associated with subjects acting on behalf of users, or "none".

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretation addresses the problem described in the Issue statement. It provides the ability to extend FIA_USB with a new component that provides the ability to specify the rules that govern attribute inheritance between users and subjects. It also makes explicit the listing of attributes to be inherited.

I-0353: Association Of Access Control Attributes With Subjects And Objects

NUMBER: I-0353
STATUS: Formally Superseded
TYPE: NIAP Interpretation

TITLE: Association Of Access Control Attributes With Subjects And Objects
SUPERSEDED BY:
I-0416 Association Of Access Control Attributes With Subjects And Objects

EFFECTIVE DATE: 2000-03-27
SUPERSEDED ON: 2000-12-05

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 6.2 FDP_ACF.1
CC v2.1 Part 2 Subclause F.2 FDP_ACF.1
RELATED TO:
I-0354 Association Of Information Flow Attributes W/Subjects And Information
CCIMB ENTRY: CCIMB-INTERP-0103

STATEMENT OF INTERPRETATION:

The following interprets the FDP_ACF.1 component:

Access Control Policies shall provide a clear association of controlled entities (subjects, objects) with relevent security attributes.

SPECIFIC INTERPRETATION:

To address this interpretation, the FDP_ACF.1.1 element should be reworded to the following (additions marked thusly; deletions marked thusly):

> FDP_ACF.x.1: The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following types of subject and object security attributes: [assignment: security attributes, named groups of security attributes *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes or named groups of SFP-relevant security attributes*]

In the Part 2 Annex (Section F.1), the second paragraph for the assignment operation for FDP_ACF.1.1 should be reworded as:

> In FDP_ACF.x.1, the PP/ST should specify, for each type of controlled subject and object, the security attributes and/or named groups of security attributes that the function will use in the specification of the rules. For example,...*[remainder of existing wording]*.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

The CC wording for FDP_ACF.1.1 is unclear when it refers to an assignment of "security attributes, named groups of security attributes":

- This is unclear in that it seems to call for a simple list of security attributes, without association of security attributes to the controlled entities.

This interpretation corrects this problem. It makes it clear that an appropriate assignment is one that provides, for each controlled entity, the SFP-relevant security attributes of that entity. This can be clearly provided as a two column table: one column is the controlled entity (subject, information), the other is a list of SFP-relevant security attributes for that controlled entity.

I-0354: Association Of Information Flow Attributes W/Subjects And Information

NUMBER: I-0354
STATUS: Formally Superseded
TYPE: NIAP Interpretation

TITLE: Association Of Information Flow Attributes W/Subjects And Information
SUPERSEDED BY:
I-0417 Association Of Information Flow Attributes W/Subjects And Information

EFFECTIVE DATE: 2000-03-27
SUPERSEDED ON: 2000-12-11

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 6.6 FDP_IFF
CC v2.1 Part 2 Subclause F.6 FDP_IFF
RELATED TO:
I-0353 Association Of Access Control Attributes With Subjects And Objects
CCIMB ENTRY: CCIMB-INTERP-0104,CCIMB-INTERP-0105

STATEMENT OF INTERPRETATION:

The following interprets the FDP_IFF.1 and FDP_IFF.2 components:

Information Flow Control Policies shall provide a clear association of controlled entities (subjects, information) with relevent security attributes.

SPECIFIC INTERPRETATION:

To address this interpretation, the FDP_IFF.1.1 and FDP_IFF.2.1 elements should be reworded to the following (additions marked thusly; deletions marked thusly):

> FDP_IFF.x.1: The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes *list of subjects and information controlled under the indicated SFP, and for each, the SFP-relevant security attributes*]

In the Part 2 Annex (Section F.6), the second paragraph for the assignment operation for both FDP_IFF.1.1 and FDP_IFF.2.1 should be replaced with:

> In FDP_IFF.x.1, the PP/ST should specify, for each type of controlled subject and information, the security attributes that are relevant to the specification of the SFP rules. For example, such security attributes may be things such the subject identifier, subject sensitivity label, subject clearance label, information sensitivity label, etc. The types of security attributes should be sufficient to support the

environmental needs.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

The CC wording for FDP_IFF.1.1 and FDP_IFF.1.2 is confusing and unclear when it refers to an assignment of "the minimum number and type of security attributes":

- This is confusing in the area of "minimum number"; the annex fails to clarify this when it refers to a "minimum number...to support the environmental needs".
- This is unclear in that it seems to call for a simple list of security attributes, without association of security attributes to the controlled entities.

This interpretation corrects this problem. It makes it clear that an appropriate assignment is one that provides, for each controlled entity, the SFP-relevant security attributes of that entity. This can be clearly provided as a two column table: one column is the controlled entity (subject, information), the other is a list of SFP-relevant security attributes for that controlled entity.

I-0355: Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3

NUMBER: I-0355
STATUS: Formally Superseded
TYPE: NIAP Interpretation

TITLE: Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3
SUPERSEDED BY:
I-0418 Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3

EFFECTIVE DATE: 2000-03-27
SUPERSEDED ON: 2000-12-05

SOURCE REFERENCE: CC v2.1 Part 1 Subclause C.2.9
CC v2.1 Part 3 Subclause 5.8 ASE_TSS
RELATED TO: <None>

STATEMENT OF INTERPRETATION:

The following interprets the ASE_TSS requirements in their interaction with the Part 1 (Annex C) specification of the TOE Summary Specification:

The Part 1 Annex C specification of the TOE Summary Specification is a more complete list of requirements than is found in the ASE_TSS elements in Part 3.

SPECIFIC INTERPRETATION:

To address this interpretation, the following elements should be added to Part 3:

- **ASE_TSS.1.11C**: The TOE summary specification shall demonstrate that the strength of TOE function claims made are valid, or demonstrate that assertions that such claims are unnecessary are valid.
- **ASE_TSS.1.12C**: The TOE summary specification rationale shall be presented at a level of detail that matches the level of detail of the definition of security functions.

Additionally, new work units for ASE_TSS should be created in the CEM to address any new Content and Presentation of Evidence elements.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

The goal of the ASE_TSS elements is to capture the requirements stated in the normative text in Part 1, Section C.2.9. For the most part, this is true. However, there are two requirements in Section C.2.9 that are not completely captured in

ASE_TSS.

Part 1, Section C.2.9 says:

> c) The TOE summary specification rationale shall show that the TOE security functions and assurance measures are suitable to meet the TOE security requirements.
>
> The following shall be demonstrated:
>
> 1) that the combination of specified TOE IT security functions work together so as to satisfy the TOE security functional requirements;
>
> 2) that the strength of TOE function claims made are valid, or that assertions that such claims are unnecessary are valid.
>
> 3) that the claim is justified that the stated assurance measures are compliant with the assurance requirements.
>
> The statement of rationale shall be presented at a level of detail that matches the level of detail of the definition of the security functions.

The first sentence of C.2.9 "c)" is verbatim in ASE_TSS.1.5C. Item 1 is stated in ASE_TSS.1.6C. Item 2 doesn't appear in ASE_TSS. Item 3 appears in ASE_TSS.1.8C. The last paragraph of C.2.9 "c)" is not addressed in ASE_TSS.

Thus, there are two portions of Part 1 that are not addressed in Part 3: C.2.9 "c)2)" and the second paragraph of C.2.9 "c)". This interpretation brings the Part 3 requirements on the TOE Summary Specification into agreement with the Part 1 normative material.

I-0362: Scope Of Permitted Refinements

NUMBER: I-0362
STATUS: Approved by TTAP/CCEVS Management
TYPE: NIAP Interpretation

TITLE: Scope Of Permitted Refinements

EFFECTIVE DATE: 2000-03-27

SOURCE REFERENCE: CC v2.1 Part 1 Subclause 4.4.1.3
CC v2.1 Part 2 Subclause 2.1.4.4
CEM v1.0 Part 2 Subclause 4.4.6 ASE_REQ

RELATED TO:
I-0394 Iteration Must Cover All Scopes

CCIMB ENTRY: CCIMB-INTERP-0106

STATEMENT OF INTERPRETATION:

The following provides clarification for Part 1, Section 4.4.1.3, with respect to Permitted Operations on Components:

Refinements always have the characteristic that a TOE meeting the refined requirement would also meet the unrefined requirement.

SPECIFIC INTERPRETATION:

In order to address this interpretation, the following changes should be made to CC V2.1:
(Additions marked thusly; deletions marked thusly)

- In Part 1, Section 4.4.1.3, under "Permitted operations on components", reword item "d)" as follows:

  d) **refinement**, which permits the addition of extra detail when the component is used. Refinements always have the characteristic that a TOE meeting the refined requirement would also meet the unrefined requirement.

- In Part 2, Section 2.1.4.4, "Refinement", add to the end of the first paragraph:

> Refinement always has the characteristic that a TOE meeting the refined requirement would also meet the unrefined requirement.

The CEM v1.0 already incorporates this definition of refinement in ASE_REQ.1-12; however, it should be reviewed to ensure that additional changes are not required.

PROJECTED IMPACT:

Some existing PPs/STs may use refinement incorrectly.

SUPPORT:

This interpretation provides the specific criteria changes to capture the definition of refinement used in CCIMB-INTERP-0015b and in the CEM. As such, it brings the CC into agreement with the CEM.

The underlying notion of refinement is that of narrowing. There are two types of narrowing possible:

- **Narrowing of Implementation**. In this form of narrowing, the PP/ST author would restrict the set of acceptable implementations in some way. Such a narrowing would always meet the unrefined requirement, and would never create additional dependencies.
- **Narrowing of Scope**. In this form of narrowing, the PP/ST author limits the application of the requirement to some subset of what is called out or implied by the unrefined requirement. For example, the scope might be narrowed from the entire TOE to a specific SFP or type of system entry. Narrowing of scope results in a TOE where the unrefined requirement is not met in all cases.

This interpretation limits refinement to narrowing of implementation. If narrowing of scope is required, an explicitly stated IT security requirement must be used. Thus, the use of refinement in crafting requirements is extremely limited.

Note that refinment may be used to clarify meaning or grammar, as long as the change still meets the definition of a proper refinement.

Refinement is acceptable both for functional and assurance requirements. Refinement in the case of assurance might be a narrowing of procedure or paradigm; that is, restricting developers or testers to the use of a specific development or testing paradigm of the many potential paradigms acceptable under the requirements.

I-0363: Attribute Inheritance/Modification Rules Need To Be Included In Policy

NUMBER: I-0363
STATUS: Approved by TTAP/CCEVS Management
TYPE: NIAP Interpretation

TITLE: Attribute Inheritance/Modification Rules Need To Be Included In Policy

EFFECTIVE DATE: 2000-03-27

SOURCE REFERENCE: CC v2.1 Part 2 Annex F FDP
CC v2.1 Part 2 Clause 6 FDP
RELATED TO: <None>
CCIMB ENTRY: CCIMB-INTERP-0107

STATEMENT OF INTERPRETATION:

The following interprets the entire FDP class in its interaction with the FMT_MSA.1 element:

> FMT_MSA.1.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles].

Rules relating to modification and inheritance of security attributes are part of a Security Function Policy.

SPECIFIC INTERPRETATION:

To address this interpretation, a new family (FDP_ATR, Security Attribute Policy), should be added to the FDP Class. This family should contain the following component:

> **FDP_ATR.1 Security Attribute Management and Inheritance**
>
> FDP_ATR.1.1. As part of the [assignment: access control SFP, information flow control SFP], the TSF shall enforce the following policy rules with respect to security attribute establishment: [assignment: list of rules governing security attribute inheritance]
>
> FDP_ATR.1.2. As part of the [assignment: access control SFP, information flow control SFP], the TSF shall enforce the following policy rules with respect to security attribute modification: [assignment: list of rules governing security attribute modification]
>
> Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow

control]

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

FMT_MSA.1.1 only allows the specification of the roles permitted to make selected security attribute modifications. However, the FMT_MSA component provides no ability to specify policies related to security attribute modification, such as how new objects inherit security attributes from creating subjects, or ancillary rules that control security attribute modification. For example, one cannot use FMT_MSA to specify a rule that a Mandatory Access Control SFPs policy must be satisfied in order to set security attributes controlled under a Discretionary Access Control policy.

One might think that such rules could be specified under FDP_ACF or FDP_ICF. However, those families allow specification of rules related to access of objects, not how security attributes obtain values. Providing a place to specify such rules appears to be an omission in the CC. This interpretation corrects that omission.

I-0364: Application Notes In Protection Profiles Are Informative Only

NUMBER: I-0364
STATUS: Approved by TTAP/CCEVS Management
TYPE: NIAP Interpretation

TITLE: Application Notes In Protection Profiles Are Informative Only

EFFECTIVE DATE: 2000-03-27

SOURCE REFERENCE: CC v2.1 Part 1 Subclause B.2.7
CC v2.1 Part 3 Clause 4 APE
RELATED TO: <None>
CCIMB ENTRY: CCIMB-INTERP-0108

STATEMENT OF INTERPRETATION:

The following interprets Section B.2.7 of Part 1, which states:

> B.2.7 Application notes
>
> This optional section may contain additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE.

Application Notes are not normative; they provide information only.

SPECIFIC INTERPRETATION:

To address this interpretation, the following paragraph should be added to Part 1, Section B.2.7.:

> Application notes should not contain normative information; rather, they should provide additional clarification or guidance information. It should be clear to what document element (e.g., threats, objectives, component elements) the application note applies, and the application note should be consistent with that document element.

To make Part 3 consistent with Part 1, the following should be added to the APE class:

> Application Notes (APE_APP)
>
> **Objectives**
>
> Application Notes, if present, provide additional clarification or guidance information with respect to document elements (e.g., threats, objectives, component elements) of the PP.
>
> **APE_APP.1 Application Note Requirements**
>
> Dependencies: No Dependencies

Developer Action Elements:

None, as application notes are optional.

Content and Presentation Elements:

APE_APP.1.1C Application notes, if provided, shall be informative only.

APE_APP.1.2C Application notes, if provided, shall be consistent with the specific elements of the PP to which they apply.

Evaluator Action Elements:

APE_APP.1.1E The evaluator shall confirm that any provided application notes meet all requirements for content and presentation of evidence.

There should be corresponding changes in the CEM to reflect the new Part 3 component.

PROJECTED IMPACT:

Some existing PPs may contain application notes with normative or inconsistent material.

SUPPORT:

The words in Part 1, Section B.2.7 are potentially misleading with respect to application notes, as the phrase "useful for the ... evaluation" has been read by some to allow normative material in application notes. However, for functional elements, the application notes are contained in the Part 2 Annex, which states at the beginning of the annex:

> This annex contains informative guidance for the families and components found in the main body of Part 2, which may be required by users, developers or evaluators to use the components.

Further, Section A.1.2 of the Part 2 Annex clearly notes that any user or evaluator notes are informative (A.1.2.2, A.1.2.3). Section A.1.3.2 notes that the application notes at the component level are "additional refinement in terms of narrative qualification as it pertains to a specific component." Refinement of an informative section can never be normative.

This leads to the conclusion that application notes are informative *only*, and that any normative material should be expressed through predefined components, refinements of predefined components (such as to specify a specific method of implementation) or explicitly specified requirements.

Further, application notes should not contradict the document element to which they apply. For example, it would be confusing to an evaluator or developer to have an element require only passwords, and the associated application discuss the use of non-password biometric devices. A larger scope of consistency analysis is not required due to transitivity: if the note is consistent with its associated element, and that element is consistent with the remainder of the PP (when called for in the APE requirements), then the application note should be similarly consistent.

Application notes are unique in Part 1, Annex B in that they are not explicitly mentioned in any other document area, and that they are optional. However, practice has allowed them to appear in other document areas. As such, the easiest way to address application notes in Part 3 was to create a new family to address application notes, wherever they may appear.

I-0370: Clarification Of ``Audit Records''

NUMBER:	I-0370
STATUS:	Formally Superseded
TYPE:	NIAP Interpretation
TITLE:	Clarification Of ``Audit Records''
SUPERSEDED BY:	
I-0422	Clarification Of ``Audit Records''
EFFECTIVE DATE:	2000-03-27
SUPERSEDED ON:	2000-12-05
SOURCE REFERENCE:	CC v2.1 Part 2 Subclause 3.6 FAU_STG
	CC v2.1 Part 2 Subclause C.6 FAU_STG
RELATED TO:	
I-0371	Some Modifications To The Audit Trail Are Authorized
CCIMB ENTRY:	CCIMB-INTERP-0109

STATEMENT OF INTERPRETATION:

The following interprets the .1 and .2 elements of the FAU_STG.1 and FAU_STG.2 components:

In general, the phrase "audit records" in these elements refers to audit records stored in the "audit trail," as described in the Part 2 Annex. However, the use of the phrase "audit records" in this way does not preclude the actions specified as acceptable in FAU_STG.2.3, FAU_STG.3, and FAU_STG.4.

SPECIFIC INTERPRETATION:

The application notes in the Part 2 Annex for FAU_STG.2 should be clarified to indicate that the use of the term "audit records", in most cases, refers to the entire trail except when a specific subset must be addressed (as in FAU_STG.2.3, FAU_STG.3.*, and FAU_STG.4.*).

The elements for FAU_STG.1.* and FAU_STG.2.* should be modified to add the phrase "in the audit trail" after "audit records" in all elements.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretation arises because a confusion is introduced due to the Part 2 usage of the term "Audit Records" as opposed to the term "Audit Trail". The Part 2 Annex, Section C.6, clarifies by implication that the term "Audit Records" refers to the records in the audit trail, as the application notes refer almost exclusively to the "audit trail" or the records in the trail.

The problem is that the current CC Part 2 words are potentially misleading; in particular, FAU_STG.1.2 and FAU_STG.2.2 could be read so as to allow an authorized administrator to modify specific audit records. This appears not to be what was desired.

However, there is a rationale for the use of the term "audit records": it is used in Part 2 to permit truncation of an audit trail (i.e., deletion of some of the records from the trail). Further, there may be the need to permit some assigned action to address a subset of the records in the trail. As a result, it would be inappropriate to simply substitute "audit trail" for "audit records".

I-0371: Some Modifications To The Audit Trail Are Authorized

NUMBER: I-0371
STATUS: Formally Superseded
TYPE: NIAP Interpretation

TITLE: Some Modifications To The Audit Trail Are Authorized
SUPERSEDED BY:
I-0423 Some Modifications To The Audit Trail Are Authorized

EFFECTIVE DATE: 2000-03-27
SUPERSEDED ON: 2000-12-11

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 3.6 FAU_STG
CC v2.1 Part 2 Subclause C.6 FAU_STG
RELATED TO:
I-0370 Clarification Of ``Audit Records''

STATEMENT OF INTERPRETATION:

The following interprets the following elements in FAU_STG:

> FAU_STG.1.2 The TSF shall be able to [selection: prevent, detect] modifications to the audit records.
>
> FAU_STG.2.2 The TSF shall be able to [selection: prevent, detect] modifications to the audit records.

Only unauthorized modifications are prohibited. Modifications to audit records performed in accordance with TSF policy are permitted.

SPECIFIC INTERPRETATION:

To address this interpretation, the Part 2 elements FAU_STG.1.2 and FAU_STG.2.2 should be modified to insert "unauthorised" before "modifications".

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretation brings the elements into conformance with the words in the Part 2 Annex, by making it explicit that only unauthorized modifications are to be prohibited.

Note that the ability to perform authorised modifications of the audit data is a management function addressed by FMT_MTD.1; these changes would be auditable in accordance with the audit section of FMT_MTD.1.

I-0373: FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical

NUMBER:	I-0373
STATUS:	Formally Superseded
TYPE:	NIAP Interpretation
TITLE:	FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical
SUPERSEDED BY:	
I-0424	FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical
EFFECTIVE DATE:	2000-03-27
SUPERSEDED ON:	2000-12-05
SOURCE REFERENCE:	CC v2.1 Part 2 Subclause 10.11 FPT_SEP CC v2.1 Part 2 Subclause J.11 FPT_SEP
RELATED TO:	<None>
CCIMB ENTRY:	CCIMB-INTERP-0110

STATEMENT OF INTERPRETATION:

The following interprets the entire FPT_SEP family:

FPT_SEP.2 and FPT_SEP.3 permit some or all access control and information flow SFPs to be in a distinct domain and are not hierarchical.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes should be made to FPT_SEP: (additions marked thusly; deletions marked thusly):

- FPT_SEP.2.3 should be changed to: " ... in a security domains for ..."
- FPT_SEP.3.3 should be changed to: "... in a security domains for their own..."
- A new component, FPT_SEP.4, should be created that is the same as FPT_SEP.3, except that element FPT_SEP.4.3 should be changed to: " ... each in a security domain for its ..."
- The hierarchy should be modified so that both FPT_SEP.2 and FPT_SEP.3 are hierarchical to FPT_SEP.1, and the new component FPT_SEP.4 is hierarchical to both FPT_SEP.2 and

FPT_SEP.3.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

According to Section 2.1.2.3 in Part 2, "A component is hierarchical to another if it offers more security." The problem is that FPT_SEP.2, depending on the instantiation, does not necessarily provide less security than FPT_SEP.3. It could be instantiated to provide the same security as FPT_SEP.3. Hence, FPT_SEP.3 cannot be hierarchical to FPT_SEP.2.

To correct this problem, adjust the hierarchy to make FPT_SEP.3 hierarchical to FPT_SEP.1, not FPT_SEP.2. To make clear that placing each access control and information flow SFP into a separate domain provides more security than having two or more SFPs in a single domain, an additional component is added that is hierarchical to both FPT_SEP.2 and FPT_SEP.3 that has each SFP in its own domain.

This change further corrects the inconsistency between CC Part 2 and the CC Part 2 Annex in making clear that FPT_SEP.2 and FPT_SEP.3 may have more than a single domain for the SFPs.

Note that both components (FPT_SEP.2 and FPT_SEP.3) allow for distinct domains per SFP, and that both components are silent with respect to non-data protection SFPs.

I-0375: Elements Requiring Authentication Mechanism

NUMBER: I-0375
STATUS: Approved by TTAP/CCEVS Management and Posted
TYPE: NIAP Interpretation

TITLE: Elements Requiring Authentication Mechanism
APPROVAL POSTING: [cc-in 00019]

EFFECTIVE DATE: 2001-03-15

SOURCE REFERENCE: CC v2.1 Part 2 Subclause G.4 FIA_UAU
RELATED TO: <None>

ISSUE:

PP/ST authors should be able to specify the authentication mechanisms that a TOE must supply. This is easily done by using FIA_UAU.5 when there are multiple authentication mechanisms. When there is only one authentication mechanism, however, the CC words do not make it clear how the PP/ST author is to specify the authentication mechanism.

STATEMENT OF INTERPRETATION:

For interfaces that use a single authentication mechanism, the authentication mechanism is specified through refinement of FIA_UAU.1.2 or FIA_UAU.2.1.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1 Part 2:

- In Subclause G.4, FIA_UAU.1, "Operations", the following text is added:

  Refinement:

  FIA_UAU.1.2 should be refined to indicate any specific TSF mechanism that must be used for authentication. This levies a requirement on the TSF to provide the specified authentication mechanism.

Iteration:

The FIA_UAU.1 component can be iterated, with each iteration changing FIA_UAU.1.2 to provide distinct authentication mechanisms for distinct user interfaces, as long as all user interfaces to the TSF are addressed.

- In Subclause G.4, FIA_UAU.2, an "Operations" section is added, consisting of the following paragraphs:

  Refinement:

  FIA_UAU.2.1 should be refined to indicate any specific TSF mechanism that must be used for authentication. This levies a requirement on the TSF to provide the specified authentication mechanism.

  Iteration:

  The FIA_UAU.2 component can be iterated, with each iteration changing FIA_UAU.2.1 to provide distinct authentication mechanisms for distinct user interfaces, as long as all user interfaces to the TSF are addressed.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretation addresses the ISSUE by using the approach of refining FIA_UAU.1.2 or FIA_UAU.2.1 to indicate the method of authentication that must be used (e.g., "...to be successfully authenticated using a TSF-provided password mechanism..."). Such a refinement implies that the TSF must provide the indicated mechanism.

Additionally, the CC is unclear on how to handle differing authentication mechanisms for different interfaces (e.g., multiple-use passwords on internal network connections and single-use passwords for external accesses). This interpretation provides clarification that iteration to address individual interfaces is the appropriate manner of specification. For example, FIA_UAU.1 might be iterated to require passwords for external connections, but biometric authentication for local connections.

I-0377: Settable Failure Limits Are Permitted

NUMBER:	I-0377
STATUS:	Formally Superseded
TYPE:	NIAP Interpretation
TITLE:	Settable Failure Limits Are Permitted
SUPERSEDED BY:	
I-0425	Settable Failure Limits Are Permitted
EFFECTIVE DATE:	2000-03-27
SUPERSEDED ON:	2000-12-05
SOURCE REFERENCE:	CC v2.1 Part 2 Subclause 7.1 FIA_AFL CC v2.1 Part 2 Subclause G.1 FIA_AFL
RELATED TO:	<None>
CCIMB ENTRY:	CCIMB-INTERP-0111

STATEMENT OF INTERPRETATION:

The following interprets FIA_AFL.1.1:

The number of unsuccessful authentication attempts is permitted to be specifiable by an administrator.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes should be made to FIA_AFL.1.1: (additions marked thusly, deletions marked thusly)

> FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: positive integer number], "an authorized administrator configurable integer"] unsuccessful authentication attempts occur related to [assignment: list of authentication events].

Additionally, corresponding changes should be made in the Part 2 Annex for FIA_AFL to reflect the changes in the terms used in the assignment.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

The Part 2 Annex for FIA_AFL says, for the assignment:

> In FIA_AFL.1.1, if the PP/ST author should specify the default number of unsuccessful authentication attempts that, when met or surpassed, will trigger the events. The PP/ST author may specify that the number is: "an authorised administrator configurable number".

This is reasonable; the PP/ST author may wish to allow the number to be adjusted dynamically by an authorised administrator. However, the wording used ("[assignment: number]") does not allow a phrase to be inserted. This interpretation permits the phrase.

This interpretation also addresses an ambiguity in the original words. "Number", as used in the element, could potentially be real or negative. That is inappropriate; it it more precise to call it a positive integer.

I-0383: Content Of PP Claims Rationale

NUMBER:	I-0383
STATUS:	Formally Superseded
TYPE:	NIAP Interpretation
TITLE:	Content Of PP Claims Rationale
SUPERSEDED BY:	
I-0426	Content Of PP Claims Rationale
EFFECTIVE DATE:	2000-03-27
SUPERSEDED ON:	2000-12-05
SOURCE REFERENCE:	CC v2.1 Part 1 Subclause C.2.9 CC v2.1 Part 3 Subclause 5.5 ASE_PPC
RELATED TO:	<None>
CCIMB ENTRY:	CCIMB-INTERP-0114

STATEMENT OF INTERPRETATION:

The following interprets the ASE_PPC requirements in their interaction with the Part 1 (Annex C) specification of the PP Claims Rationale:

The Part 1 Section C.2.9 "d)" specification of the PP Claims Rationale is a more complete list of requirements than is found in the ASE_PPC elements in Part 3.

SPECIFIC INTERPRETATION:

To address this interpretation, a new Content and Presentation element should be added to the ASE_PPC.1 component:

> ASE_PPC.1.xC: The PP Claims Rationale shall explain any difference between the ST security objectives and requirements and those of any PP to which conformance is claimed.

Additional work units should be added to the CEM to address this new content and presentation element.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretation addresses an omission in the Common Criteria. Part 1 Section C.2.9 "d)" specifies the required content for the PP claims rationale, but this was never captured in Part 3.

I-0385: Identification Of Standards

NUMBER: I-0385
STATUS: Approved by TTAP/CCEVS Management
TYPE: NIAP Interpretation

TITLE: Identification Of Standards

EFFECTIVE DATE: 2000-03-27

SOURCE REFERENCE: CC v2.1 Part 3 Subclause 4.5 APE_REQ
CC v2.1 Part 3 Subclause 5.6 ASE_REQ
RELATED TO: <None>
CCIMB ENTRY: CCIMB-INTERP-0115

STATEMENT OF INTERPRETATION:

The following interprets both the APE_REQ and ASE_REQ families in Part 3 of the Common Criteria:

Claims about use of a standard must be unambiguous with respect to the source of a metric and the meaning of compliance. If a compliance claim is made, the PP/ST author must provide an indication of how compliance is to be determined.

SPECIFIC INTERPRETATION:

To address this intepretation, the following elements should be added to the Content and Presentation elements of APE_REQ.1, with parallel additions to the Content and Presentation elements of ASE_REQ.1:

> APE_REQ.1.xC: All requirements that claim compliance with an external standard shall be unambiguous with respect to the source of the metric and the meaning of compliance.
>
> APE_REQ.1.xC: All requirements that claim compliance with an external standard shall stipulate how compliance is ascertained.

For these units, an application note should be added along the lines of the following:

> In some instances, it is appropriate for a PP/ST to claim compliance with an external standard, such as the definition of an encryption algorithm. When the standards

document provides only one mode of operation of the algorithm, or level of use of the algorithm, this is not a problem. However, some standards define multiple approaches, and a simple citation is insufficient. Citations of an external standard should be unambiguous with respect to what is being required. If the standards specifies multiple modes or manners of operations, the citation should be specific enought to determine which mode or manner of operation applies to the TSF.

Additionally, there are many ways of determining compliance with a standard. It may be performed as part of the TOE evaluation, it might be a developer claim, or it might be verified by an independent party. In order to have consistency across evaluations, the PP/ST author should specify the means of determining compliance, so that consistency of interpretation across all uses of the PP/ST is achieved.

Additional work units should be added to the CEM to address these new elements.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

In some instances, it is appropriate for a PP/ST to claim compliance with an external standard, such as the definition of an encryption algorithm. When the standards document provides only one mode of operation of the algorithm, or level of use of the algorithm, this is not a problem. However, some standards define multiple approaches, and a simple citation is insufficient. This interpretation requires citations of an external standard to be unambiguous with respect to what is being required. If the standards specifies multiple modes or manners of operations, the citation must be specific enought to determine which mode or manner of operation applies to the TSF.

Additionally, there are many ways of determining compliance with a standard. It may be performed as part of the TOE evaluation, it might be a developer claim, or it might be verified by an independent party. In order to have consistency across evaluations, the PP/ST author should specify the means of determining compliance, so that consistency of interpretation across all uses of the PP/ST is achieved.

I-0389: Recovery To A Known State

NUMBER:	I-0389
STATUS:	Approved by TTAP/CCEVS Management and Posted
TYPE:	NIAP Interpretation
TITLE:	Recovery To A Known State
APPROVAL POSTING:	[cc-in 00022]
EFFECTIVE DATE:	2001-03-15
SOURCE REFERENCE:	CC v2.1 Part 2 Subclause 10.8 FPT_RCV CC v2.1 Part 2 Subclause J.8 FPT_RCV
RELATED TO:	
I-0406	Automated Or Manual Recovery Is Acceptable

ISSUE:

There are situations where some form of recovery from a known backup is required, but there is no formal model to argue that the known state is provably secure.

STATEMENT OF INTERPRETATION:

It must be possible to recover to a known previous state, as opposed to one that is provably secure.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1, Part 2: (additions marked thusly; deletions marked thusly)

- The following component is added to the FPT_RCV family in Subclause 10.8. This component would be immediately below the current lowest component in the existing FPT_RCV hierarchy:

  FPT_RCV.NIAP-0389-1 Recovery to Known State

  Hierarchical to: No other components.

  FPT_RCV.NIAP-0389-1.1 For [selection: [assignment: *list of failures/service discontinuities*], *"no failures/service discontinuities"*], the TSF shall ensure the

return of the TOE to a previously known state using automated procedures.

FPT_RCV.NIAP-0389-1.2 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a previously known state is provided.

Dependencies:

AGD_ADM.1 Administrator guidance

- In Subclause 10.8, rework the component levellings to make FPT_RCV.2-NIAP-0406 immediately hierarchical to the new component.
- In Clause 10, Figure 10.1, the class decomposition figure is updated to show that component 2-NIAP-0406 is immediately hierarchical to component NIAP-0389-1.
- In Subclause 10.8, add the following after the "Component Levelling" diagram:

  FPT_RCV.NIAP-0389-1 Recovery to a Known State, allows a TOE to only provide mechanisms that involve human intervention to a previously known, but not provably secure, state.
- In Subclause 10.8, FPT_RCV.2-NIAP-0406, change the "Hierarchical To:" as follows:

  Hierarchical To: No other components FPT_RCV.NIAP-0389-1
- In Subclause J.8, add the following after paragraph 1236:

  FPT_RCV.NIAP-0389-1 Recovery to a Known State

  In the hierarchy of the trusted recovery family, recovery that recovers only to a previously known state, as opposed to known secure state, is the least desirable.

  User Application Notes

  This component is intended for use in TOEs that do not require recovery to a known secure state. The requirements of this component reduce the threat of protection compromise resulting from an attended TOE returning to an unknown state after recovery from a failure or other discontinuity.

  Evaluator application notes

  It is acceptable for the functions that are available to an authorised user for trusted recovery to be available only in a maintenance mode. Controls should be in place to limit access during maintenance to authorised users.

  If "no failures/service discontinuities" is selected for FPT_RCV.NIAP-0389.1, this means that there are no explicitly mandated discontinuities for which automated recovery must be provided. The TOE developer always has the option to provide an automated recovery mechanism for a discontinuity.

  Operations

  Selection:

If there are no explicit situations for which automated recovery is mandated, "no failures/service discontinuities" should be selected in FPT_RCV.NIAP-0389-1.1. Otherwise, the assignment should be selected to provide the list of failures or other discontinuities for which automated recovery must be possible.

It is acceptable for a PP author to complete only the selection and leave the assignment open, so as to indicate that the list of discontinuities for which automated recovery is required must be non-empty.

Assignment:

For FPT_RCV.NIAP-0389-1.1, the PP/ST author should specify the list of failures or other discontinuities for which automated recovery must be possible.

- In Annex J, Figure J.1, the class decomposition figure is updated to show that component 2-NIAP-0406 is immediately hierarchical to component NIAP-0389-1.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

The words in the annex for FPT_RCV state:

> Throughout this family, the phrase "secure state" is used. This refers to some state in which the TOE has consistent TSF data and a TSF that can correctly enforce the policy. This state may be the initial "boot" of a clean system, or it might be some checkpointed state. The "secure state" is defined in the TSP model. If the developer provided a clear definition of the secure state and the reason why it should be considered secure, the dependency from FPT_FLS.1 to ADV_SPM.1 can be argued away.

Although this allows a secure state to be a previously checkpointed state, this ability is buried. This component makes it explicit; it also makes it clear that a previously known state may or may not be a secure state.

Note: This interpretation is being applied to the CC as modified by I-0406.

I-0393: A Completely Evaluated ST Is Not Required When TOE Evaluation Starts

NUMBER: I-0393
STATUS: Approved by TTAP/CCEVS Management and Posted
TYPE: NIAP Interpretation

TITLE: A Completely Evaluated ST Is Not Required When TOE Evaluation Starts
APPROVAL POSTING: [cc-in 00021]

EFFECTIVE DATE: 2001-03-15

SOURCE REFERENCE: CC v2.1 Part 1 Figure 4.4
CC v2.1 Part 1 Figure 5.1
CC v2.1 Part 1 Subclause 4.2.2
CC v2.1 Part 1 Subclause 4.5.3
CC v2.1 Part 3 Subclause 3.1
RELATED TO: <None>

ISSUE:

In an ideal world, a Security Target (ST) would be completely evaluated before a TOE evaluation starts. In order for this to happen, however, there would need to be a finalized TOE configuration (down to version and patch numbers), and no aspects of evaluation (including testing) would result in changes to the TOE.

In the real world, this never happens. Instead, there may be nuances of the hardware or software platform that are finalized during the TOE evaluation. Further, the evaluation activities, such as testing and analysis, may uncover areas where the ST requires correction, especially in the TOE summary specification.

STATEMENT OF INTERPRETATION:

A completely-evaluated ST is not required before TOE evaluation may start, although a substantially complete ST is required.

SPECIFIC INTERPRETATION:

In order to address this interpretation, the following changes are made to CC v2.1, Part 1 (additions marked thusly; deletions marked thusly):

- Correct Figure 4.4 to change the circle labeled "Evaluate TOE" to "Evaluate ST and TOE".

- Reword Subclause 4.2.2, paragraph 110, as follows:

  The TOE evaluation process, as described in Figure 4.4 may be carried out in parallel with development, or it may follow. The process of TOE evaluation includes the evaluation of the ST against the ASE requirements in Part 3. The principal inputs to TOE evaluation are:

  a) the set of TOE evidence, which includes the evaluated a substantially complete ST as the basis for TOE evaluation (a "substantially complete" ST is an ST where all sections have been completed to an extent acceptable by the evaluation scheme and for which no significant evaluation hurdles are foreseen);

  b) the TOE for which the evaluation is required;

  c) the evaluation criteria, methodology, and scheme.

- Reword Subclauses 4.5.2 and 4.5.3 as follows:

  4.5.2 ST TOE evaluation

  TOE evaluation involves two tasks: evaluation of an ST against the ST evaluation criteria contained in Part 3, and evaluation of the TOE against the evaluation criteria in Part 3 using the ST as a basis.

  The evaluation of the ST for the TOE is carried out against the evaluation criteria for STs contained in Part 3. The goal of such an evaluation is twofold: first to demonstrate that the ST is complete, consistent, and technically sound and hence suitable for use as the basis for the corresponding TOE evaluation; second, in the case where an ST claims conformance to a PP, to demonstrate that the ST properly meets the requirements of the PP.

  4.5.3 TOE evaluation

  The TOE evaluation is carried out against the evaluation criteria contained in Part 3 using an evaluated the ST as the basis. The goal of such an evaluation is to demonstrate that the TOE meets the security requirements contained in the ST. The TOE evaluation may commence against a ST that is substantially complete, provided that the ST evaluation is fully complete prior to completion of the TOE evaluation.

- Change all references in the CC to subclause 4.5.3 to refer instead to subclause 4.5.2.
- Correct Figure 5.1 to have the arrow go from the "Evaluated PP" square to the current "Evaluate TOE" circle, the latter being relabeled as "Evaluate ST and TOE". The "Evaluate ST" circle and the "ST evaluation results" rectangle would be eliminated.

In order to address this interpretation, the following changes are made to CC v2.1, Part 3 (additions marked thusly; deletions marked thusly):

- Reword Subclause 3.1, paragraph 133, as follows:

  These criteria are the first requirements presented in this Part 3 because the PP and ST evaluation will normally be performed before the TOE evaluation. They play a special role in that information about the TOE is assessed and the functional and assurance requirements are evaluated in order to find out whether the PP or ST is a meaningful basis for a TOE evaluation.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretation recognizes the real world situation. The position taken by this interpretation is supported by CEM v1.0 Section B.4.1, paragraph 1800, which says:

> For some cases the different assurance classes may recommend or even require a sequence for the related activities. A specific instance is the ST activity. The ST evaluation activity is started prior to any TOE evaluation activities since the ST provides the basis and context to perform them. However, a final verdict on the ST evaluation may not be possible until the TOE evaluation is complete, since changes to the ST may result from activity findings during the TOE evaluation.

This interpretation requires the ST to be substantially complete. This means that:

1. All sections of the ST are substantially complete.
2. A preliminary assessment of the ST against the ASE requirements uncovers no significant failures.

This interpretation does not place a specific metric on "substantially complete". The setting of such a metric, as well as defining "substantially complete", is an evaluation scheme issue. The appropriate value is a business decision that weights the risks to an evaluation's schedule against the reasonability of finalizing ST details during TOE evaluation.

I-0394: Iteration Must Cover All Scopes

NUMBER:	I-0394
STATUS:	Approved by TTAP/CCEVS Management and Posted
TYPE:	NIAP Interpretation
TITLE:	Iteration Must Cover All Scopes
APPROVAL POSTING:	[cc-in 00012]
EFFECTIVE DATE:	2000-12-20
SOURCE REFERENCE:	CC v2.1 Part 2 Subclause 2.1.4.1 CEM v1.0 Part 2 Subclause 3.4.5 APE_REQ.1 CEM v1.0 Part 2 Subclause 4.4.6 ASE_REQ.1
RELATED TO:	
I-0397	Iteration On Assurance Components/Elements
I-0362	Scope Of Permitted Refinements
CCIMB ENTRY:	CCIMB-INTERP-0138

ISSUE:

The question of "narrowing of scope" (i.e., limiting the applicability of an element) has recently been debated as to whether it is an acceptable refinement. The approach taken in CCIMB-INTERP-0097/0098 indicates that it is not. However, the CEM provides a situation in which iteration can be used to narrow scope. It is not clear from the CC and the CEM that all aspects of a requirement must be covered.

STATEMENT OF INTERPRETATION:

If iteration is used to narrow applicability to a portion of the TOE, the collection of all the iterations must cover all aspects of the requirement.

SPECIFIC INTERPRETATION:

To address this intepretation, CC v2.1 Part 2 Subclause 2.1.4.1, paragraph 75 is reworded as follows (additions marked thusly; deletions marked thusly):

> Where necessary to cover different aspects of the same requirement (e.g. identification

> of more than one type of user), repetitive use of the same component from this part of the CC to cover each aspect is permitted. If iteration is used to narrow the applicability, the collection of all iterations of the same requirement must cover all aspects.

The following change is made to both CEM v1.0 Part 2 Section 3.4.5 APE_REQ.1-11 Paragraph 225 "d)" and CEM v1.0 Part 2 Section 4.4.6 ASE_REQ.1-12 Paragraph 415 "d)": (additions marked thusly; deletions marked thusly):

> d) for an iteration, that each iteration of a component is different from each other iteration of that component (at least one element of a component is different from the corresponding element of the other component), or that the component applies to a different part of the TOE. In the latter case, there must be sufficient iterations that all aspects of the requirement are covered.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

Narrowing of scope is clearly not the intent of iteration. CC v2.1 Part 2 Subclause 2.1.4.1, says:

> Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use of the same component from this part of the CC to cover each aspect is permitted.

The key part of this is "to cover each aspect". This implies that all aspects of the requirement must be covered by the collection of the iterations. Making that particular characteristic of iteration clear is the goal of this interpretation.

I-0395: Security Attributes Include Attributes Of Information And Resources

NUMBER:	I-0395
STATUS:	Approved by TTAP/CCEVS Management and Posted
TYPE:	NIAP Interpretation
TITLE:	Security Attributes Include Attributes Of Information And Resources
APPROVAL POSTING:	[cc-in 00020]
EFFECTIVE DATE:	2001-03-15
SOURCE REFERENCE:	CC v2.1 Part 1 Subclause 2.3
RELATED TO:	
I-0351	User Attributes To Be Bound Should Be Specified

ISSUE:

There is a discrepancy between the definition of "Security attribute" in Part 1 and the use of the term in other portions of the CC, where security attributes are referred to in the context of information and resources.

STATEMENT OF INTERPRETATION:

The term "security attribute" also applies to security-related characteristics associated with information (under an information flow policy) and resources.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1, Part 1: (additions marked thusly; deletions marked thusly)

- Subclause 2.3, paragraph 46 is changed as follows:

  Security attribute--Information associated with Characteristics of subjects, users, and/or objects, information, and/or resources that is used for the enforcement of the TSP.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

The modification of this definition extends the definition of "security attribute" to "information" (as used in FDP_IFC and FDP_IFF) and resources. The definition is also changed to eliminate using the term "information" in two different contexts.

I-0397: Iteration On Assurance Components/Elements

NUMBER: I-0397
STATUS: Approved by TTAP/CCEVS Management and Posted
TYPE: NIAP Interpretation

TITLE: Iteration On Assurance Components/Elements
APPROVAL POSTING: [cc-in 00018]

EFFECTIVE DATE: 2001-03-15

SOURCE REFERENCE: CC v2.1 Part 1 Subclause 4.4.1
CC v2.1 Part 3 Subclause 2.1.3.5
CC v2.1 Part 3 Subclause 2.1.4
RELATED TO: <None>

ISSUE:

The CC, in Part 1, appears to permit iteration at the level of assurance components. However, Part 3 only discusses refinement at the element level; no mention is made of iteration.

STATEMENT OF INTERPRETATION:

Iteration is permitted on sets of assurance elements (as defined in Part 3, Section 2.1.3.5) and on assurance elements.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1, Part 3: (additions marked thusly; deletions marked thusly)

- In Section 2.1.3.5, after paragraph 53, add the following paragraph:

  Iteration is permitted at the level of developer action elements, content and presentation of evidence elements, and explicit evaluator action elements.

- In Section 2.1.4, replace paragraph 56 with the following:

> In contrast to CC Part 2, neither assignment nor selection operations are relevant for elements in CC Part 3; however, refinements and iterations may be made to Part 3 elements as required.

FURTHER CONSIDERATIONS:

The criteria changes may be subject to further changes depending on the resolution of I-0379 (Documentation Sections) [an RFI sent to the CCIMB]; in particular, assigment may move from the not-relevant category to being relevent when explicitly specified.

Additionally, the above paragraph may be subject to futher changes depending on the resolution of I-0394 (Iteration Must Cover All Scopes); in particular, there may be additional words noting that if iteration is used to apply a requirement to a subpart of the TOE, there must be sufficient iterations that the entire TOE is covered.

Lastly, corresponding methodology changes may be needed to address the effects of these changes.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretation corrects the identified discrepancy.

There are three potential levels of iteration for assurance components:

1. At the level of the entire component.
2. At the level of a set of assurance elements (C/D/E).
3. At the element level.

It is difficult to come up with an example of iteration of an entire assurance component that does not result in unnecessary redundancy. It is more appropriate to iterate assurance at either the level of the D/C/E groupings, or at the level of individual elements. For example:

1. Iteration at the level of D/C/E might be useful for independent testing, if the ST author wanted to have multiple groups performing independent testing. In such a case, the "E" components might be iterated to explicitly specify the groups performing testing.
2. Iteration at the element level might be useful for indicating that some elements of a design description might have an additional formal specification in addition to the level called out by the EAL.

I-0405: American English Is An Acceptable Refinement

NUMBER: I-0405
STATUS: Approved by TTAP/CCEVS Management and Posted
TYPE: NIAP Interpretation

TITLE: American English Is An Acceptable Refinement
APPROVAL POSTING: [cc-in 00006]

EFFECTIVE DATE: 2000-12-20

SOURCE REFERENCE: CEM v1.0 Part 2 Subclause 3.4.5 APE_REQ
CEM v1.0 Part 2 Subclause 4.4.6 ASE_REQ
RELATED TO: <None>
CCIMB ENTRY: CCIMB-INTERP-0139

ISSUE:

The language used in a PP/ST should not distract or confuse the reader. Constant shifts between U.S. and International English spelling could do just that.

STATEMENT OF INTERPRETATION:

It is acceptable to refine Common Criteria elements to use a consistent spelling convention (i.e., U.S. English or International English) with a single global identification.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CEM v1.0 Part 2: (additions marked thusly; deletions marked thusly)

- Subclause 3.4.5.2.1, Action APE_REQ.1.1E, Work Unit APE_REQ.1-11, para 225, item "c)", 3rd paragraph is modified as follows:

  A special case of refinement is an editorial refinement, where a small change is made in a requirement, i.e. rephrasing a sentence due to adherence to proper English grammar or changing the element to use a consistent spelling convention

(U.S. English or International English). This change is not allowed to modify the meaning of the requirement in any way.

- Subclause 3.4.5.2.1, Action APE_REQ.1.1E, Work Unit APE_REQ.1-11, para 225, item "c)", last paragraph is modified as follows:

  The evaluator is reminded that editorial refinements have to be clearly identified (see work unit APE_REQ.1-10). It is acceptable for editorial refinements for the purposes of achieving a consistent spelling style to be identified once (at the start of the enumeration of the requirements), so as not to clutter the requirements presentation.

- Subclause 4.4.6.3.1, Action ASE_REQ.1.1E, Work Unit ASE_REQ.1-12, para 415, item "c)", 3rd paragraph is modified as follows:

  A special case of refinement is an editorial refinement, where a small change is made in a requirement, i.e. rephrasing a sentence due to adherence to proper English grammar or changing the element to use a consistent spelling convention (U.S. English or International English). This change is not allowed to modify the meaning of the requirement in any way.

- Subclause 4.4.6.3.1, Action ASE_REQ.1.1E, Work Unit ASE_REQ.1-12, para 415, item "c)", last paragraph is modified as follows:

  The evaluator is reminded that editorial refinements have to be clearly identified (see work unit ASE_REQ.1-10). It is acceptable for editorial refinements for the purposes of achieving a consistent spelling style to be identified once (at the start of the enumeration of the requirements), so as not to clutter the requirements presentation.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretations permits a PP/ST author to use a consistant spelling style with a single global identification.

I-0406: Automated Or Manual Recovery Is Acceptable

NUMBER:	I-0406
STATUS:	Approved by TTAP/CCEVS Management and Posted
TYPE:	NIAP Interpretation
TITLE:	Automated Or Manual Recovery Is Acceptable
APPROVAL POSTING:	[cc-in 00023]
EFFECTIVE DATE:	2001-03-15
SOURCE REFERENCE:	CC v2.1 Part 2 Subclause 10.8 FPT_RCV CC v2.1 Part 2 Subclause J.8 FPT_RCV
RELATED TO:	
I-0389	Recovery To A Known State

ISSUE:

The current CC v2.1 FPT_RCV.1 elements are worded in such a fashion as to preclude the use of automated mechanisms when manual recovery is to be supported. This is an unlikely situation; a PP/ST author may not care whether recovery is automated or manual.

STATEMENT OF INTERPRETATION:

Either manual or automated recovery systems are acceptable. The PP/ST author has the discretion to specify for what recovery scenarios automated recovery is appropriate, and for what recovery scenarios manual recovery is appropriate.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1, Part 2: (additions marked thusly; deletions marked thusly)

- In Clause 10.8, delete the existing FPT_RCV.1. As a result of this, Paragraph 415 and the "Management" section for FPT_RCV.1 are deleted; FPT_RCV.1 is removed from the "Audit" header between paragraphs 421 and 422, the "Component levelling" figure is modified to

delete component 1, and the component decomposition figures (Clause 10, Figure 10.1 and Clause J, Figure J.1) showing the levelling structure for FPT are corrected to eliminate component 1. Additionally, the annex material for FPT_RCV.1 is deleted.

- FPT_RCV.2 is relabeled as FPT_RCV.2-NIAP-0406. Unless otherwise noted in these changes, all normative and informative material associated with FPT_RCV.2 is incorporated unchanged into FPT_RCV.2-NIAP-0406, and all references to FPT_RCV.2 in the CC, CEM, or other Common Criteria documentation is changed to refer to FPT_RCV.2-NIAP-0406.
- FPT_RCV.3 is relabeled as FPT_RCV.3-NIAP-0406. Unless otherwise noted in these changes, all normative and informative material associated with FPT_RCV.3 is incorporated unchanged into FPT_RCV.3-NIAP-0406, and all references to FPT_RCV.3 in the CC, CEM, or other Common Criteria documentation is changed to refer to FPT_RCV.3-NIAP-0406.
- The "Class Decomposition" figure in Clause 10, Figure 10.1 is modified to show component 2-NIAP-0406 as the first hierarchical component off of FPT_RCV, with component 3-NIAP-0406 immediately hierarchical to 2-NIAP-0406.
- The "Component Levelling" figure in Subclause 10.8 is modified to show component 2-NIAP-0406 as the first hierarchical component off of FPT_RCV, with component 3-NIAP-0406 immediately hierarchical to 2-NIAP-0406.
- Subclause 10.8, Paragraph 416 is replaced with the following:

  FPT_RCV.2-NIAP-0406 Automated recovery Recovery from Failure, provides, for at least one type of service discontinuity, a specific list (possibly empty) of discontinuities for which the TSF must provide the capability for recovery to a secure state without human intervention; recovery for other discontinuities may require human intervention.

- Subclause 10.8, Paragraph 417 is replaced with the following:

  FPT_RCV.3-NIAP-0406 Automated recovery Recovery without undue loss, also provides for automated recovery from failure, but strengthens the requirements by disallowing undue loss of protected objects.

- In Clause 10.8, the following changes are made to FPT_RCV.2:

  FPT_RCV.2-NIAP-0406 Automated recovery Recovery from Failure

  Hierarchical To: FPT_RCV.1 No Other Components

  FPT_RCV.2.21-NIAP-0406 For [selection: [assignment: *list of failures/service discontinuities*], *"no failures/service discontinuities"*], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

  FPT_RCV.2.12-NIAP-0406 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

- In Clause 10.8, the following changes are made to FPT_RCV.3:

  FPT_RCV.3-NIAP-0406 Automated recovery Recovery without undue loss

  Hierarchical To: FPT_RCV.2-NIAP-0406

FPT_RCV.3.21-NIAP-0406 For [selection: [assignment: *list of failures/service discontinuities*], *"no failures/service discontinuities"*], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.3.12-NIAP-0406 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

- The "Class Decomposition" figure in Annex J, Figure J.1 is modified to show component 2-NIAP-0406 as the first hierarchical component off of FPT_RCV, with component 3-NIAP-0406 immediately hierarchical to 2-NIAP-0406.
- In Subclause J.8, the application notes for FPT_RCV.2 are modified as follows:

FPT_RCV.2-NIAP-0406 Automated recovery Recovery from Failure

This component requires the TSF to provide mechanisms for automated or manual recovery. Automated recovery is considered to be more useful than manual recovery, as it allows the machine to operate in an unattended fashion. However, there may be situations where the list of discontinuities that required automated recovery is not known in advance, or the PP/ST author does not want to mandate automated recovery.

User Application Notes

The component FPT_RCV.2 extends the feature coverage of FPT_RCV.1 by requiring that there be at least one automated method of recovery from failure or service discontinuity. It addresses the threat of protection compromise resulting from an unattended TOE returning to an insecure state after recovery from a failure or other discontinuity.

FPT_RCV.2-NIAP-0406 addresses the threat of protection compromise resulting from a TOE returning to an insecure state after recover from a failure or other discontinuity. It provides the ability for unattended recovery for anticipated discontinuities.

Evaluator application notes

It is acceptable for the functions that are available to an authorised user for trusted recovery to be available only in a maintenance mode. Controls should be in place to limit access during maintenance to authorised users.

For FPT_RCV.2.12-NIAP-0406, it is the responsibility of the developer of the TSF to determine the set of recoverable failures and service discontinuities.

If "no failures/service discontinuities" is selected for FPT_RCV.2.1-NIAP-0406, this means that there are no explicitly mandated discontinuities for which automated recovery must be provided. The TOE developer always has the option to provide an automated recovery mechanism for a discontinuity.

It is assumed that the robustness of the automated recovery mechanisms will be verified.

Operations

Selection:

If there are no explicit situations for which automated recovery is mandated, "no failures/service discontinuities" should be selected in FPT_RCV.2.1-NIAP-0406. Otherwise, the assignment should be selected to provide the list of failures or other discontinuities for which automated recovery must be possible.

It is acceptable for a PP author to complete only the selection and leave the assignment open, so as to indicate that the list of discontinuities for which automated recovery is required must be non-empty.

Assignment:

For FPT_RCV.2.21-NIAP-0406, the PP/ST author should specify the list of failures or other discontinuities for which automated recovery must be possible.

- In Subclause J.8, the application notes for FPT_RCV.3 are modified as follows:

  FPT_RCV.3-NIAP-0406 Automated recovery Recovery without undue loss

  This component requires the TSF to provide mechanisms for automated or manual recovery. Automated recovery is considered to be more useful than manual recovery, as it allows the machine to operate in an unattended fashion, but it runs the risk of losing a substantial number of objects. Preventing undue loss of objects provides additional utility to the recovery effort.

  User Application Notes

  The component FPT_RCV.3-NIAP-0406 extends the feature coverage of FPT_RCV.2-NIAP-0406 by requiring that there not be undue loss of TSF data or objects within the TSC. At FPT_RCV.2-NIAP-0406, the automated recovery mechanisms could conceivably recover by deleting all objects and returning the TSF to a known secure state. This type of drastic automated recovery is precluded in FPT_RCV.3-NIAP-0406.

  This component addresses the threat of protection compromise resulting from an unattended TOE returning to an insecure state after recovery from a failure or other discontinuity with a large loss of TSF data or objects within the TSC.

  Evaluator application notes

  It is acceptable for the functions that are available to an authorised user for trusted recovery to be available only in a maintenance mode. Controls should be in place to limit access during maintenance to authorised users.

  For FPT_RCV.3.12-NIAP-0406, it is the responsibility of the developer of the

TSF to determine the set of recoverable failures and service discontinuities.

If "no failures/service discontinuities" is selected for FPT_RCV.3.1-NIAP-0406, this means that there are no explicitly mandated discontinuities for which automated recovery must be provided. The TOE developer always has the option to provide an automated recovery mechanism for a discontinuity.

It is assumed that the evaluators will verify the robustness of the automated recovery mechanisms.

Operations

Selection:

If there are no explicit situations for which automated recovery is mandated, "no failures/service discontinuities" should be selected in FPT_RCV.3.1-NIAP-0406. Otherwise, the assignment should be selected to provide the list of failures or other discontinuities for which automated recovery must be possible.

It is acceptable for a PP author to complete only the selection and leave the assignment open, so as to indicate that the list of discontinuities for which automated recovery is required must be non-empty.

Assignment:

For FPT_RCV.3.21-NIAP-0406, the PP/ST author should specify the list of failures or other discontinuities for which automated recovery must be possible.

For FPT_RCV.3.3, the PP/ST author should provide a quantification for the amount of loss of TSF data or objects that is acceptable.

FURTHER CONSIDERATIONS:

Other families and components in Part 2 should be examined to correct any dependency references to components in FPT_RCV.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This reworking of the FPT_RCV elements makes it so that automated mechanisms are permitted in all cases, or the PP/ST author has the option of indicating the specific situations in which automated recovery is mandated.

I-0411: Guidance Includes AGD_ADM, AGD_USR, ADO, And ALC_FLR

NUMBER: I-0411
STATUS: Approved by TTAP/CCEVS Management and Posted
TYPE: NIAP Interpretation

TITLE: Guidance Includes AGD_ADM, AGD_USR, ADO, And ALC_FLR
APPROVAL POSTING: [cc-in 00007]

EFFECTIVE DATE: 2000-12-22

SOURCE REFERENCE: CC v2.1 Part 1 Subclause 2.3
CC v2.1 Part 3 Clause 11 AGD
RELATED TO: <None>
CCIMB ENTRY: CCIMB-INTERP-0140

ISSUE:

Many CC requirements refer simply to administrator and user guidance, which in the strict reading, would refer only to those documents called out in AGD_ADM and AGD_USR. However, this guidance should also include delivery instructions; installation, generation, and startup instructions; and flaw remediation guidance.

STATEMENT OF INTERPRETATION:

User and Administrative Guidance includes ADO and ALC_FLR guidance documentation as well as AGD_USR, AGD_ADM.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1, Part 1: (additions marked thusly; deletions marked thusly)

- In Subclause 2.3, the definition of Target of Evaluation is replaced with the following:

  Target of Evaluation (TOE)--An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

- The following new term is added to the glossary in CC v2.1 Part 1 Subclause 2.3:

  Guidance Documentation--Guidance documentation includes user and administrator guidance and, when included in a PP or ST, the specific guidance for users and administrators resulting from the requirements in the ADO class and the ALC_FLR family.

Additionally, the following changes are made to CC v2.1, Part 3: (additions marked thusly; deletions marked thusly)

- In Clause 11, paragraph 370, the following text is appended:

  > Guidance documentation includes user and administrator guidance and, when included in a PP or ST, the specific guidance for users and administrators resulting from the requirements in the ADO class and the ALC_FLR family.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretation is simply a straight-forward application of the concept captured in CCIMB-INTERP-0094. While CCIMB-INTERP-0094 has ALC_FLR as the subject, that interpretation focuses on the concept of guidance documentation being AGD plus input from other CC components.

I-0416: Association Of Access Control Attributes With Subjects And Objects

NUMBER: I-0416
STATUS: Approved by TTAP/CCEVS Management and Posted
TYPE: NIAP Interpretation

TITLE: Association Of Access Control Attributes With Subjects And Objects
SUPERSEDES:
I-0353 Association Of Access Control Attributes With Subjects And Objects
APPROVAL POSTING: [cc-in 00011]

EFFECTIVE DATE: 2000-12-05

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 6.2 FDP_ACF.1
CC v2.1 Part 2 Subclause F.2 FDP_ACF.1
RELATED TO:
I-0353 Association Of Access Control Attributes With Subjects And Objects
I-0354 Association Of Information Flow Attributes W/Subjects And Information
I-0417 Association Of Information Flow Attributes W/Subjects And Information
CCIMB ENTRY: CCIMB-INTERP-0103

ISSUE:

The Common Criteria does not currently provide functional requirements for identifying the clear association of controlled entities (subjects, information) with relevant security attributes. The existing FDP_ACF family provides only for a simple list of security attributes, without the ability to describe the required association to controlled entities.

STATEMENT OF INTERPRETATION:

The CC is modified so that the statement of Access Control Policy provides a clear association of controlled entities (subjects, objects) with relevant security attributes.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1, Part 2: (additions marked thusly; deletions marked thusly):

- The FDP_ACF.1 component is relabeled as FDP_ACF.1-NIAP-0416. Unless otherwise noted in these changes, all normative and informative material associated with FDP_ACF.1 is incorporated unchanged into

FDP_ACF.1-NIAP-0416, and all references to FDP_ACF.1 in the CC, CEM, or other Common Criteria documentation is changed to refer to FDP_ACF.1-NIAP-0416.

- The FDP_ACF.1.1 element is replaced with FDP_ACF.1.1-NIAP-0416, as follows:

  FDP_ACF.1.1-NIAP-0416: The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

- In Subclause F.2, the first sentence in paragraph 763 is replaced with:

  In FDP_ACF.1.1-NIAP-0416, the PP/ST author should specify, for each controlled subject and object, the security attributes and/or named groups of security attributes that the function will use in the specification of the rules.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretation makes it clear that an appropriate assignment is one that provides, for each controlled entity, the SFP-relevant security attributes of that entity. This can be clearly provided as a two column table: one column is the controlled entity (subject, object), the other is a list of SFP-relevant security attributes for that controlled entity.

Note: This interpretation is superseding a previously-approved formal interpretation primarily to reflect modifications to the interpretation format. The intent of the interpretation has not been changed, although some specifics of the criteria changes or the support may have been clarified or corrected.

I-0417: Association Of Information Flow Attributes W/Subjects And Information

NUMBER: I-0417
STATUS: Approved by TTAP/CCEVS Management and Posted
TYPE: NIAP Interpretation

TITLE: Association Of Information Flow Attributes W/Subjects And Information
SUPERSEDES:
I-0354 Association Of Information Flow Attributes W/Subjects And Information
APPROVAL POSTING: [cc-in 00016]

EFFECTIVE DATE: 2000-12-11

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 6.6 FDP_IFF.1.1
CC v2.1 Part 2 Subclause 6.6 FDP_IFF.2.1
CC v2.1 Part 2 Subclause F.6 FDP_IFF
RELATED TO:
I-0353 Association Of Access Control Attributes With Subjects And Objects
I-0354 Association Of Information Flow Attributes W/Subjects And Information
I-0416 Association Of Access Control Attributes With Subjects And Objects
CCIMB ENTRY: CCIMB-INTERP-0104

ISSUE:

The Common Criteria does not currently provide functional requirements for identifying the clear association of controlled entities (subjects, information) with relevant security attributes. The existing FDP_IFF family provides only for a simple list of security attributes, without the ability to describe the required association to controlled entities.

STATEMENT OF INTERPRETATION:

The CC is modified so that the statement of Information Flow Control Policy provides a clear association of controlled entities (subjects, information) with relevant security attributes.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1: (additions marked thusly; deletions marked thusly):

- The FDP_IFF.1 component is relabeled as FDP_IFF.1-NIAP-0417. Unless otherwise noted in these changes, all

normative and informative material associated with FDP_IFF.1 is incorporated unchanged into FDP_IFF.1-NIAP-0417, and all references to FDP_IFF.1 in the CC, CEM, or other Common Criteria documentation is changed to refer to FDP_IFF.1-NIAP-0417.

- The FDP_IFF.1.1 element is replaced with FDP_IFF.1.1-NIAP-0417, as follows:

  FDP_IFF.1.1-NIAP-0417: The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *the minimum number and type of security attributes list of subjects and information controlled under the indicated SFP, and for each, the SFP-relevant security attributes*]

- The FDP_IFF.2 component is relabeled as FDP_IFF.2-NIAP-0417. Unless otherwise noted in these changes, all normative and informative material associated with FDP_IFF.2 is incorporated unchanged into FDP_IFF.2-NIAP-0417, and all references to FDP_IFF.2 in the CC, CEM, or other Common Criteria documentation is changed to refer to FDP_IFF.2-NIAP-0417.
- The FDP_IFF.2.1 element is replaced with FDP_IFF.2.1-NIAP-0417, as follows:

  FDP_IFF.2.1-NIAP-0417: The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *the minimum number and type of security attributes list of subjects and information controlled under the indicated SFP, and for each, the SFP-relevant security attributes*]

- Part 2, Subclause F.6, paragraph 810 is replaced by:

  In FDP_IFF.1.1-NIAP-0417, the PP/ST author should specify the minimum number and types of security attributes that the function will use in specify, for each type of controlled subject and information, the security attributes that are relevant to the specification of the SFP rules. For example, such security attributes may be things such the subject identifier, subject sensitivity label, subject clearance label, information sensitivity label, etc. The minimum number of each type types of security attributes should be sufficient to support the environmental needs.

- Part 2, Subclause F.6, paragraph 822 is replaced by:

  In FDP_IFF.2.1-NIAP-0417, the PP/ST should specify the minimum number and types of security attributes that the function will use in specify, for each type of controlled subject and information, the security attributes that are relevant to the specification of the SFP rules. For example, such security attributes may be things such the subject identifier, subject sensitivity label, subject clearance label, information sensitivity label, etc. The minimum number of each type types of security attributes should be sufficient to support the environmental needs.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretation makes it clear that an appropriate assignment is one that provides, for each controlled entity, the SFP-relevant security attributes of that entity. This might be provided as a two column table: one column is the controlled entity (subject, information), the other is a list of SFP-relevant security attributes for that controlled entity.

Note: This interpretation is superseding a previously-approved formal interpretation primarily to reflect modifications to the interpretation format. The intent of the interpretation has not been changed, although some specifics of the criteria changes or the support may have been clarified or corrected.

I-0418: Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3

NUMBER:	I-0418
STATUS:	Approved by TTAP/CCEVS Management and Posted
TYPE:	NIAP Interpretation
TITLE:	Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3
SUPERSEDES:	
I-0355	Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3
APPROVAL POSTING:	[cc-in 00009]
EFFECTIVE DATE:	2000-12-05
SOURCE REFERENCE:	CC v2.1 Part 1 Subclause C.2.9 CC v2.1 Part 3 Subclause 5.8 ASE_TSS
RELATED TO:	
I-0355	Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3
CCIMB ENTRY:	CCIMB-INTERP-0105

ISSUE:

The goal of the ASE_TSS elements is to capture the requirements stated in the normative text in Part 1, Subclause C.2.9. For the most part, this is true. However, there are two requirements in Section C.2.9 that are not completely captured in ASE_TSS: C.2.9 "c)2)" and the second paragraph of C.2.9 "c)".

STATEMENT OF INTERPRETATION:

All requirements on the TOE Summary Specification specified in the CC v2.1 Part 1 Annex C specification of the TOE Summary Specification apply.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1, Part 3:

- ASE_TSS.1 is relabeled as ASE_TSS.1-NIAP-0418. Unless otherwise noted in these changes, all normative and informative material associated with ASE_TSS.1 is incorporated unchanged into ASE_TSS.1-NIAP-0418, and all references to ASE_TSS.1 in the CC, CEM, or other Common Criteria documentation is changed to refer to ASE_TSS.1-NIAP-0418.
- The following elements are added to ASE_TSS.1-NIAP-0418 in order to bring it into agreement with Part 1, Subclause C.2.9:

  ASE_TSS.1.NIAP-0418-1C: The TOE summary specification shall demonstrate that the strength of TOE function claims made are valid, or demonstrate that assertions that such claims are unnecessary are valid.

  ASE_TSS.1.NIAP-0418-2C: The TOE summary specification rationale shall be presented at a level of detail that matches the level of detail of the definition of security functions.

FURTHER CONSIDERATIONS:

Corresponding methodology changes are needed to address the new Content and Presentation of Evidence elements in ASE_TSS.1-NIAP-0418.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

CC v2.1 Part 1, Subclause C.2.9 says:

> c) The TOE summary specification rationale shall show that the TOE security functions and assurance measures are suitable to meet the TOE security requirements.
>
> The following shall be demonstrated:
>
> 1) that the combination of specified TOE IT security functions work together so as to satisfy the TOE security functional requirements;
>
> 2) that the strength of TOE function claims made are valid, or that assertions that such claims are unnecessary are valid.
>
> 3) that the claim is justified that the stated assurance measures are compliant with the assurance requirements.
>
> The statement of rationale shall be presented at a level of detail that matches the level of detail of the definition of the security functions.

The first sentence of C.2.9 "c)" is verbatim in ASE_TSS.1.5C. Item 1 is stated in ASE_TSS.1.6C. Item 2 doesn't appear in ASE_TSS. Item 3 appears in ASE_TSS.1.8C. The last paragraph of C.2.9 "c)" is not addressed in ASE_TSS.

Thus, there are two portions of Part 1 that are not addressed in Part 3: C.2.9 "c)2)" and the second paragraph of C.2.9 "c)".

This interpretation brings the Part 3 requirements on the TOE Summary Specification into agreement with the Part 1 normative material.

Note: This interpretation is superseding a previously-approved formal interpretation primarily to reflect modifications to the interpretation format. The intent of the interpretation has not been changed, although some specifics of the criteria changes or the support may have been clarified or corrected.

I-0422: Clarification Of ``Audit Records''

NUMBER:	I-0422
STATUS:	Approved by TTAP/CCEVS Management and Posted
TYPE:	NIAP Interpretation
TITLE:	Clarification Of ``Audit Records''
SUPERSEDES:	
I-0370	Clarification Of ``Audit Records''
APPROVAL POSTING:	[cc-in 00008]
EFFECTIVE DATE:	2000-12-05
SOURCE REFERENCE:	CC v2.1 Part 2 Subclause 3.6 FAU_STG
	CC v2.1 Part 2 Subclause C.6 FAU_STG
RELATED TO:	
I-0370	Clarification Of ``Audit Records''
I-0371	Some Modifications To The Audit Trail Are Authorized
I-0423	Some Modifications To The Audit Trail Are Authorized
CCIMB ENTRY:	CCIMB-INTERP-0109

ISSUE:

There is a confusion introduced with the Part 2 usage of the term "Audit Records", as opposed to the term "Audit Trail". The Part 2 Annex, Section C.6, clarifies by implication that the term "Audit Records" refers to the records in the audit trail, as the application notes refer almost exclusively to the "audit trail" or the records in the trail. The problem with the use of the term "audit records" is that audit records may appear outside the audit trail, for example, after they have been retrieved through a selection.

STATEMENT OF INTERPRETATION:

In the .1 and .2 elements of the FAU_STG.1 and FAU_STG.2 components, the phrase "audit records" refers to audit records stored in the "audit trail," as described in the Part 2 Annex. However, the use of the phrase "audit records" in this way does not preclude the actions specified as acceptable in FAU_STG.2.3, FAU_STG.3, and FAU_STG.4.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to the CC v2.1, Part 2: (additions marked thusly; deletions marked thusly)

- FAU_STG.1 is relabeled as FAU_STG.1-NIAP-0422. Unless otherwise noted in these changes, all

normative and informative material associated with FAU_STG.1 is incorporated unchanged into FAU_STG.1-NIAP-0422, and all references to FAU_STG.1 in the CC, CEM, or other Common Criteria documentation is changed to refer to FAU_STG.1-NIAP-0422.

- The elements in FAU_STG.1 are replaced with the following elements:

  FAU_STG.1.1-NIAP-0422: The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

  FAU_STG.1.2-NIAP-0422: The TSF shall be able to [selection: *prevent, detect*] modifications to the audit records in the audit trail.

- FAU_STG.2 is relabeled as FAU_STG.2-NIAP-0422. Unless otherwise noted in these changes, all normative and informative material associated with FAU_STG.2 is incorporated unchanged into FAU_STG.2-NIAP-0422, and all references to FAU_STG.2 in the CC, CEM, or other Common Criteria documentation is changed to refer to FAU_STG.2-NIAP-0422.
- Elements FAU_STG.2.1 and FAU_STG.2.2 are replaced with the following elements:

  FAU_STG.2.1-NIAP-0422: The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

  FAU_STG.2.2-NIAP-0422: The TSF shall be able to [selection: *prevent, detect*] modifications to the audit records in the audit trail.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

The term "audit records" is used in Part 2 to permit truncation of an audit trail (i.e., deletion of some of the records from the trail). Further, there may be the need to permit some assigned action to address a subset of the records in the trail. As a result, it would be inappropriate to simply substitute "audit trail" for "audit records".

Note: This interpretation is superseding a previously-approved formal interpretation primarily to reflect modifications to the interpretation format. The intent of the interpretation has not been changed, although some specifics of the criteria changes or the support may have been clarified or corrected.

I-0423: Some Modifications To The Audit Trail Are Authorized

NUMBER: I-0423
STATUS: Approved by TTAP/CCEVS Management and Posted
TYPE: NIAP Interpretation

TITLE: Some Modifications To The Audit Trail Are Authorized
SUPERSEDES:
I-0371 Some Modifications To The Audit Trail Are Authorized
APPROVAL POSTING: [cc-in 00014]

EFFECTIVE DATE: 2000-12-11

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 3.6 FAU_STG
CC v2.1 Part 2 Subclause C.6 FAU_STG
RELATED TO:
I-0371 Some Modifications To The Audit Trail Are Authorized
I-0370 Clarification Of ``Audit Records''
I-0422 Clarification Of ``Audit Records''
CCIMB ENTRY: CCIMB-INTERP-0141

ISSUE:

The FAU_STG family does not currently distinguish between authorized and unauthorized modifications to the audit records. The modification controls imposed appear to be related only to unauthorized modifications.

STATEMENT OF INTERPRETATION:

Only unauthorized modifications are prohibited. Modifications to audit records performed in accordance with TSF policy are permitted.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1, Part 2: (additions marked thusly; deletions marked thusly)

- FAU_STG.1-NIAP-0422 is relabeled as FAU_STG.1-NIAP-0423. Unless otherwise noted in these changes, all normative and informative material associated with FAU_STG.1-NIAP-0422 is incorporated unchanged into FAU_STG.1-NIAP-0423, and all references to FAU_STG.1-NIAP-0422 in the CC, CEM, or other Common Criteria documentation is changed to refer to

FAU_STG.1-NIAP-0423.

- In Subclause 3.6, FAU_STG.1.2-NIAP-0422 is replaced with the following:

  FAU_STG.1.2-NIAP-0423 The TSF shall be able to [selection: *prevent, detect*] unauthorised modifications to the audit records in the audit trail.

- In Subclause 3.6, FAU_STG.2.2-NIAP-0422 is replaced with the following:

  FAU_STG.2.2-NIAP-0423 The TSF shall be able to [selection: *prevent, detect*] unauthorised modifications to the audit records in the audit trail.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretation brings the elements into conformance with the words in the Part 2 Annex, by making it explicit that only unauthorized modifications are to be prohibited.

Note that the ability to perform authorised modifications of the audit data is a management function addressed by FMT_MTD.1; these changes would be auditable in accordance with the audit section of FMT_MTD.1.

Notes:

- In the criteria changes, International English is used for conformity with the underlying component.
- This interpretation is being applied to the CC as modified by I-0422.
- This interpretation is superseding a previously-approved formal interpretation primarily to reflect modifications to the interpretation format. The intent of the interpretation has not been changed, although some specifics of the criteria changes or the support may have been clarified or corrected.

I-0424: FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical

NUMBER:	I-0424
STATUS:	Approved by TTAP/CCEVS Management and Posted
TYPE:	NIAP Interpretation
TITLE:	FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical
SUPERSEDES:	
I-0373	FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical
APPROVAL POSTING:	[cc-in 00017]
EFFECTIVE DATE:	2000-12-05
SOURCE REFERENCE:	CC v2.1 Part 2 Clause 10 FPT_SEP CC v2.1 Part 2 Clause J FPT_SEP CC v2.1 Part 2 Subclause 10.11 FPT_SEP CC v2.1 Part 2 Subclause J.11 FPT_SEP
RELATED TO:	
I-0373	FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical
CCIMB ENTRY:	CCIMB-INTERP-0110

ISSUE:

According to Section 2.1.2.3 in Part 2, "A component is hierarchical to another if it offers more security." However, FPT_SEP.2, depending on the instantiation, does not necessarily provide less security than FPT_SEP.3. It could be instantiated to provide the same security as FPT_SEP.3. Hence, FPT_SEP.3 cannot be hierarchical to FPT_SEP.2.

STATEMENT OF INTERPRETATION:

CC v2.1 is modified so that FPT_SEP reflects a proper hierarchy.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1, Part 2: (additions marked thusly; deletions marked thusly)

- FPT_SEP.2 is relabeled as FPT_SEP.2-NIAP-0424, and FPT_SEP.3 is relabeled as FPT_SEP.3-NIAP-0424. Unless otherwise noted in these changes, all normative and informative material associated with FPT_SEP.2 is incorporated unchanged into FPT_SEP.2-NIAP-0424, and all references to FPT_SEP.2 in the CC, CEM, or other Common Criteria documentation is changed to refer to FPT_SEP.2-NIAP-0424. Similarly, all normative and informative material associated with FPT_SEP.3 is incorporated unchanged into FPT_SEP.3-NIAP-0424, and all references to FPT_SEP.3 in the CC, CEM, or other Common Criteria documentation is changed to refer to FPT_SEP.3-NIAP-0424.
- In Clause 10, Figure 10.2, the hierarchy diagram for FPT_SEP is redrawn to show that components 2-NIAP-0424 (a relabeling of 2) and 3-NIAP-0424 (a relabeling of 3) are both immediately hierarchical to component 1, and new component NIAP-0424-1 is immediately hierarchical to both 2-NIAP-0424 and 3-NIAP-0424.
- In the "Component Levelling" section of Subclause 10.11, the hierarchy diagram is redrawn to show that components 2-NIAP-0424 and 3-NIAP-0424 are both immediately hierarchical to component 1, and new component NIAP-0424-1 is hierarchical to both 2-NIAP-0424 and 3-NIAP-0424.
- Paragraphs 436 and 437 of Subclause 10.11 are modified as follows:

  FPT_SEP.2-NIAP-0424 SFP domain separation, requires that the TSF be further subdivided, with distinct domain(s) for an identified set of SFPs that act as reference monitors for their policies, and a domain for the remainder of the TSF, as well as domains for the non-TSF portions of the TOE. There may be multiple reference monitor SFPs in a single domain.

  FPT_SEP.3-NIAP-0424 Complete reference monitor, requires that there be distinct domain(s) for TSP enforcement, a domain for the remainder of the TSF, as well as domains for the non-TSF portions of the TOE. However, there may be multiple SFPs within a single domain.
- The following paragraph is added after paragraph 437:

  FPT_SEP.NIAP-0424-1 Isolated reference monitor domains, requires that there be a distinct domain for each SFP providing TSP enforcement, a domain for the remainder of the TSF, as well as domains for the non-TSF portions of the TOE.
- In Subclause 10.11, the "Management" section has FPT_SEP.NIAP-0424-1 added to the list of components for which no management actions are forseen.
- In Subclause 10.11, the "Audit" section has FPT_SEP.NIAP-0424-1 added to the list of components for which there are no auditable actions.
- In Subclause 10.11, FPT_SEP.2.3 is replaced with the following:

  FPT_SEP.2.3-NIAP-0424 The TSF shall maintain the part of the TSF related to

> [assignment: list of access control and/or information flow control SFPs] in a security domain(s) for their own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to those SFPs.

- In FPT_SEP.3-NIAP-0424, the "Hierarchical To:" statement is modified to indicate that the component is hierarchical to FPT_SEP.1, not FPT_SEP.2-NIAP-0424.
- FPT_SEP.3.3 is replaced with the following:

> FPT_SEP.3.3-NIAP-0424 The TSF shall maintain the part of the TSF that enforces the access control and/or information flow control SFPs in a security domain(s) for its their own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to the TSP.

- A new component, FPT_SEP.NIAP-0424-1, is created as follows (changes are shown against the FPT_SEP.3 component; the key change being modification of FPT_SEP.3.3 to put each SFP in a distinct security domain):

> FPT_SEP.NIAP-0424-1 Isolated Complete reference monitor domains
>
> Hierarchical to: FPT_SEP.2-NIAP-0424, FPT_SEP.3-NIAP-0424
>
> FPT_SEP.NIAP-0424-1.1 The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
>
> FPT_SEP.NIAP-0424-1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.
>
> FPT_SEP.NIAP-0424-1.3 The TSF shall maintain the each part of the TSF that enforces the an access control and/or information flow control SFPs in a security domain for its own execution that protects them it from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to the TSP.
>
> Dependencies: No dependencies

- In Clause J, Figure J.2, the hierarchy diagram for FPT_SEP is redrawn to show that components 2-NIAP-0424 and 3-NIAP-0424 are both immediately hierarchical to component 1, and new component NIAP-0424-1 is immediately hierarchical to both 2-NIAP-0424 and 3-NIAP-0424.
- In Subclause J.11, paragraph 1267 is replaced with the following:

> In order to obtain the equivalent of a reference monitor, the components FPT_SEP.2-NIAP-0424 (SFP domain separation), or FPT_SEP.3-NIAP-0424 (Complete reference monitor), or FPT_SEP.NIAP-0424-1 (Isolated reference monitor domains) from this family must be used in conjunction with FPT_RVM.1 (Non-bypassability of the TSP), and ADV_INT.3 (Minimisation of complexity). Further, if complete reference mediation is required, the

components from Class FDP User data protection must cover all objects.

- In Subclause J.11, paragraph 1273 (the "Assignment" operation for FPT_SEP.2-NIAP-0424) is replaced with the following:

  For FPT_SEP.2-NIAP-0424.3, the PP/ST author should specify the access control and/or information flow control SFPs in the TSP that should have a separate domain be in distinct domain(s).

- The following text is added after paragraph 1276 for FPT_SEP.3-NIAP-0424 (Strikeout and underlining are present to show the differences from the FPT_SEP.3 wording):

  FPT_SEP.NIAP-0424-1 Complete Isolated reference monitor domains

  The most important function provided by a TSF is the enforcement of its SFPs. This component builds upon the intentions of the previous components (FPT_SEP.2-NIAP-0424 and FPT_SEP.3-NIAP-0424) by requiring that each all access control and/or information flow control FSPs be enforced in a its own domain distinct from the remainder of the TSF and other domains. This further simplifies the design and increases the likelihood that the characteristics of a reference monitor (RM), in particular, being tamperproof, are found in the TSF.

  Evaluator application notes

  It is possible that a reference monitor in a layered design may provide functions beyond those of the SFPs. This arises out of the practical nature of layered software design. The goal should be to minimise the non-SFP related functions.

  Note that it is acceptable for the reference monitors for all included SFPs to be in a single distinct reference monitor domain, as well as having multiple reference monitor domains (each enforcing one or more SFPs). If multiple reference monitor domains for SFPs are present, it is acceptable for them to be either peers or in a hierarchical relationship.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretation corrects the identified problem by adjusting the hierarchy to make FPT_SEP.3 hierarchical to FPT_SEP.1, not FPT_SEP.2. To make clear that placing each access control and information flow SFP into a separate domain provides more security than having two or more SFPs in a single domain, an additional component is added that is hierarchical to both FPT_SEP.2 and FPT_SEP.3 that has each SFP in its own domain.

This change further corrects the inconsistency between CC Part 2 and the CC Part 2 Annex in making clear that FPT_SEP.2 and FPT_SEP.3 may have more than a single domain for the SFPs.

Note that both components (FPT_SEP.2 and FPT_SEP.3) allow for distinct domains per SFP, and that both components are silent with respect to non-data protection SFPs.

Note: This interpretation is superseding a previously-approved formal interpretation primarily to reflect modifications to the interpretation format. The intent of the interpretation has not been changed, although some specifics of the criteria changes or the support may have been clarified or corrected.

I-0425: Settable Failure Limits Are Permitted

NUMBER:	I-0425
STATUS:	Approved by TTAP/CCEVS Management and Posted
TYPE:	NIAP Interpretation
TITLE:	Settable Failure Limits Are Permitted
SUPERSEDES:	
I-0377	Settable Failure Limits Are Permitted
APPROVAL POSTING:	[cc-in 00015]
EFFECTIVE DATE:	2000-12-05
SOURCE REFERENCE:	CC v2.1 Part 2 Subclause 7.1 FIA_AFL CC v2.1 Part 2 Subclause G.1 FIA_AFL
RELATED TO:	
I-0377	Settable Failure Limits Are Permitted
CCIMB ENTRY:	CCIMB-INTERP-0111

ISSUE:

In element FIA_AFL.1.1, the PP/ST author should specify the default number of unsuccessful authentication attempts that, when met or surpassed, will cause the TSF to perform some action or actions. Part 2, Subclause G.1, paragraph 958 states that the PP/ST author may specify that the number is: "an authorised administrator configurable number". However, the wording used in element FIA_AFL.1.1 ("[assignment: number]") does not allow a phrase to be inserted.

STATEMENT OF INTERPRETATION:

The number of unsuccessful authentication attempts is permitted to be specifiable by an administrator.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1, Part 2: (additions marked thusly; deletions marked thusly)

- FIA_AFL.1 is relabeled as FIA_AFL.1-NIAP-0425. Unless otherwise noted in these changes, all normative and informative material associated with FIA_AFL.1 is incorporated unchanged into FIA_AFL.1-NIAP-0425, and all references to FIA_AFL.1 in the CC, CEM, or other Common Criteria documentation is changed to refer to FIA_AFL.1-NIAP-0425.
- FIA_AFL.1.1 is replaced by the following:

  FIA_AFL.1.1-NIAP-0425: The TSF shall detect when [selection: [assignment: positive integer number], "an authorised administrator configurable integer"] unsuccessful authentication attempts occur related to [assignment: list of authentication events].
- In Subclause G.1, FIA_AFL.1, Operations, the following is added before the "Assignment" operation:

  Selection:

  In FIA_AFL.1.1-NIAP-0425, the PP/ST author should select either the assignment of a positive integer, or the phrase "an authorised administrator configurable integer".
- In Subclause G.1, FIA_AFL.1, Operations, paragraph 958 (the first "Assignment") is replaced with the following:

  In FIA_AFL.1.1-NIAP-0425, if the assignment of a positive integer is selected, the PP/ST author should specify the default number (positive integer) of unsuccessful authentication attempts that, when met or surpassed, will trigger the events. The PP/ST author may specify that the number is: "an authorised administrator configurable number".
- Annex G.1, Paragraph 959 is modified to reference FIA_AFL.1.1-NIAP-0425, instead of FIA_AFL.1.1.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretation permits the specification of the number of unauthorised authentication attempts to be specified by the administrator.

This interpretation also addresses an ambiguity in the original words. "Number", as used in the element, could potentially be real or negative. That is inappropriate; it is more precise to call it a

positive integer.

Note: This interpretation retains the wording "authorised administrator" for conformity with the original FIA_AFL.1 and its annex material.

Note: This interpretation is superseding a previously-approved formal interpretation primarily to reflect modifications to the interpretation format. The intent of the interpretation has not been changed, although some specifics of the criteria changes or the support may have been clarified or corrected.

I-0426: Content Of PP Claims Rationale

NUMBER:	I-0426
STATUS:	Approved by TTAP/CCEVS Management and Posted
TYPE:	NIAP Interpretation
TITLE:	Content Of PP Claims Rationale
SUPERSEDES:	
I-0383	Content Of PP Claims Rationale
APPROVAL POSTING:	[cc-in 00010]
EFFECTIVE DATE:	2000-12-05
SOURCE REFERENCE:	CC v2.1 Part 1 Subclause C.2.9 CC v2.1 Part 3 Subclause 5.5 ASE_PPC
RELATED TO:	
I-0383	Content Of PP Claims Rationale
CCIMB ENTRY:	CCIMB-INTERP-0114

ISSUE:

Currently, Common Criteria Part 1 Annex C and Part 3 component ASE_PPC.1 are not consistent with respect to specification of PP Claims Rationale.

STATEMENT OF INTERPRETATION:

The Part 1 Section C.2.9 "d)" specification of the PP Claims Rationale provides a more complete list of requirements than is found in the ASE_PPC elements in Part 3.

SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1, Part 3:

- ASE_PPC.1 is relabeled as ASE_PPC.1-NIAP-0426. Unless otherwise noted in these changes, all normative and informative material associated with ASE_PPC.1 is incorporated unchanged into ASE_PPC.1-NIAP-0426, and all references to ASE_PPC.1 in the CC, CEM, or other Common Criteria documentation is changed to refer to ASE_PPC.1-NIAP-0426.
- A new Content and Presentation of Evidence element is added to the ASE_PPC.1-NIAP-0426

component:

ASE_PPC.1.NIAP-0426-1C: The PP Claims Rationale shall explain any difference between the ST security objectives and requirements and those of any PP to which conformance is claimed.

FURTHER CONSIDERATIONS:

Corresponding methodology changes are needed to address this new Content and Presentation of Evidence element.

PROJECTED IMPACT:

Negligible impact anticipated.

SUPPORT:

This interpretation addresses an omission in the Common Criteria. Part 1 Section C.2.9 "d)" specifies the required content for the PP claims rationale, but this was not captured in Part 3.

Note: This interpretation is superseding a previously-approved formal interpretation primarily to reflect modifications to the interpretation format. The intent of the interpretation has not been changed, although some specifics of the criteria changes or the support may have been clarified or corrected.

I-0378: Meaning Of Compliance Claims

```
NUMBER:                 I-0378
STATUS:                 Submitted as Request for Interpretation to CCIMB
TYPE:                   Request for Interpretation

TITLE:                  Meaning Of Compliance Claims

SOURCE REFERENCE:       CC v2.1 Part 1 Subclause 4.2.1
                        CC v2.1 Part 1 Subclause 4.3
                        CC v2.1 Part 1 Subclause C.2.8
                        CC v2.1 Part 3 Subclause 5.5 ASE_PPC
RELATED TO:             <None>
CCIMB ENTRY:            CCIMB-INTERP-0112
```

ISSUE:

There is a problem in the ASE_PPC components in their relationship with the Part 1 definition of Conformance in Section C.2.8. When ASE_PPC.1.1 says "Each PP claim shall identify the PP for which compliance is being claimed, including qualifications needed for that claim", it is unclear whether:

- Must all PP assumptions be ST assumptions?
- Must all PP threats be ST threats?
- Must all PP organizational security policies be ST organizational security policies?
- Must all PP objectives be ST objectives, and must they have the same allocation (environment vs. TOE)?

It is clear that all requirements in the PP, modulo permitted operations, must be included in the ST. It is also clear that all requirements allocated to the TSF in the PP must be allocated to the TSF in the ST (although requirements allocated to the IT environment may be reallocated to the TSF). The relationship of the other front matter for compliance, however, is not clear from the CC, and there is not a strong technical argument for or against it.

STATEMENT OF INTERPRETATION:

The statement of interpretation has not yet been determined.

SPECIFIC INTERPRETATION:

None as yet determined. I-0378 is a request for interpretation addressed to the CCIMB.

PROJECTED IMPACT:

Unknown

SUPPORT:

Discussion

The CC makes it clear in Section 4.2.1 that the TOE is developed based on the security requirements in the TOE, but that these requirements must be effective in contributing to the security objectives of consumers (Part 1, Section 4.2.1, second paragraph, as well as Figure 4.3 and Figure 4.4.). In Section 4.3.3 of Part 1 the CC makes it clear that the IT security requirements are the refinement of the security objectives. This has the implication that, if the objectives change, the requirements should change.

Part 1, Section 4.3.2 makes it clear that the security objectives are a result of the analysis of the security environment; that is, the security objectives "counter the identified threats and address identified organisational security policies and assumptions" (Part 1, Section 4.3.2, first paragraph). Further, this part of the CC make it clear that the objectives must be consistent with the stated operational aim or product purpose of the TOE, and any knowledge about the physical environment.

The focus of the protection profile in the CC is the requirements contained therein. This is made clear in Part 1, Section 4.4.2.2, which says "The PP contains a set of security requirements" and "A PP is intended to be reusable and to define TOE requirements that are known to be useful and effective in meeting the identified objectives, both for functions and assurance".

In Part 1, Section C.2.8, when talking about PP claims in a Security Target, the CC says "...make a claim that the TOE conforms with the requirements of one (or possibly more than one) PP." The focus, for the most part, in this section, is on the security requirements of the PP, and the fact that they must be consistent (modulo operations) with the requirements in the ST.

The section clearly notes that the ST may have additional objectives than the PP; these additional objectives may translate to additional requirements. The CC is also clear that the ST may restate the objectives of the PP ("The CC is not prescriptive with respect to the choice of restating or referencing PP objectives"). The CC does require that the traceability to any claimed PP be clear.

What does this traceability mean? The CC seems to presume that if the objectives are changed in some significant manner, then the resulting IT requirements will be different. An analysis has not been performed to verify that this is always the case, but it seems reasonable (especially when dealing with reallocation of requirements from the IT product to the IT environment). It is also reasonable to believe that two profiles developed for different sponsors might end up having the same requirements, as the protection objectives (without the PP authors realising it) are likely to be similar.

If the PP registry contains such profiles (i.e., different sponsors and target audiences, but compatible

requirements and objectives), then an ST might claim compliance with multiple profiles. Some of these may be for distinctly different target customers than might be accounted for in the introduction of the ST (for example, an ST for general-purpose use claiming compliance with a banking industry PP, as well as a general purpose PP). Would the traceability in such a case be clear?

Consider the following: Could two PPs with distinctly different threats, assumptions, and objectives could result in an ST with the same requirements? If such a result was possible, would it be wrong for that ST to claim compliance with both PPs? Is the traceability clear?

If the focus of traceability is on requirements, the answer is yes. If the focus is on the bigger picture, the answer is maybe. The issue is one of intent: what was the intent of the CC authors? This just isn't clear from the CC.

I-0379: How To Require User/Admin Documentation For Functional Components

NUMBER:	I-0379
STATUS:	Submitted as Request for Interpretation to CCIMB
TYPE:	Request for Interpretation
TITLE:	How To Require User/Admin Documentation For Functional Components
SOURCE REFERENCE:	CC v2.1 Part 2 CC v2.1 Part 3 Clause 11 AGD CC v2.1 Part 3 Subclause 2.1.4
DOCUMENT(S):	User Guidance; Administrator Guidance
RELATED TO:	
I-0001	Delayed Enforcement Of Authorization Change
I-0002	Delayed Revocation Of DAC Access
I-0003	Access Validation After Object Label Change
I-0004	Enforcement Of Audit Settings Consistent With Protection Goals
I-0005	Action For Audit Log Overflow
I-0020	DAC Authority For Assignment
I-0183	Restrictions On Untrusted Programs In Low Assurance Products
I-0288	Actions Allowed Before I&A
CCIMB ENTRY:	CCIMB-INTERP-0113

ISSUE:

The CC does not currently provide a clear mechanism to allow a functional component to indicate information that must be present in user or administrator guidance.

STATEMENT OF INTERPRETATION:

The statement of interpretation has not yet been determined.

SPECIFIC INTERPRETATION:

There is no concensus resolution for this problem, although there are four potential solutions:

1. Allow assignments in the Part 3 Guidance family, and provide for functional components a USER/ADMINISTRATOR GUIDANCE section, similar to the audit section, that allows specification of the information to be contained in the user/administrator guidance when the component is included in a PP/ST.
2. If provision of such information is an acceptable refinement for Class AGD, then provide in Part 2 a SUGGESTED GUIDANCE REFINEMENT section to specify the information to be contained in the user/administrator guidance when the component is included in the PP/ST. There should also be an application note for Class AGD in Part 3 indicating that specific documentation of functions that must be present in guidance documentation should be provided through refinement.
3. If provision of such information is a consequence of environmental factors, then provide a SUGGESTED

ENVIRONMENTAL CONSIDERATIONS in the Part 2 functional components to specify the environmental factors to be considered when the component is included in the PP/ST.

4. Provide explicit guidance in the CEM for the Class AGD components, indicating for each functional component what information should be present in the guidance.

PROJECTED IMPACT:

No negative effect on current evaluations; may simplify the PP/ST assembly and vetting process and may help ensure that appropriate guidance is given to administrators and users.

SUPPORT:

There are many examples of where functional components require clear guidance to the administrator or user in order for their correct operation:

- Administrator Guidance:
  - Description of when authorization changes take effect.
  - Description of when changes to security attributes take effect.
  - Description of when changes to audit parameters take effect.
  - Description of the available options when the audit trail is full.
  - Description of the impact of assigning privileges and a description of implemented privileges.
  - Description of the discontinuities from which the TSF is excepted to be able to recover.
  - Description of the potential amount of audit data that might be lost in the face of a discontinuity.
  - Description for the policy on the reuse of user identifiers.
  - Guidance on the use of programs outside the TSF when privilege is present.
  - Cautions about actions available before a product reaches its secure state.
  - Descriptions about how any output labels are to be interpreted.
- User Documentation:
  - Description of how a user controls sharing of objects under an access control policy, especially if the sharing is not under the direct control of the user.
  - Description of how a user controls sharing of objects when multiple access control or information flow policies are present.
  - Description of how a user controls sharing of objects when relevant access control policies are order-dependent.
- Both:
  - Description of the risks and responsibilities regarding removable media, in particular, how residual information must be addressed when the media is removed from an ADP system and any physical security requirements.

Some of these examples are PP/ST issues: the requirement is completed from a broad Common Criteria element, and it is up to the PP/ST author to add explicitly specified assurance elements for the additional guidance information. In such cases, the best that can be done is a note in the Part 2 annex providing suggestions as to information that might be needed in the guidance documentation, as the CC authors cannot know apriori how the assignments will be completed.

However, in other cases, it is possible to know apriori when guidance is required to complement a functional element. In such cases, it should be possible to have the Common Criteria specify, as part of the functional element, the information that must be present in guidance documentation.

This interpretation presents four possible solutions to this problem.

The first adds the ability to perform assignments solely to the guidance elements, and adds a corresponding section in the functional components to specify what information should be included in the assignment if the functional component is included in a PP/ST. A variant of this approach would be to have the section in the functional component indicate that this guidance information should be called out as an explicitly specified element. Which of these variants is better depends on

how one assesses the bias against explicitly specified elements, and whether it is felt appropriate for functional elements to call out explicitly specified assurance elements.

The second approach works only if the provision of the additional functional guidance is a valid refinement of the existing AGD components. If the guidance is a valid refinement, then this approach suggests adding a list of suggested assurance refinements to the functional components.

The third approach is based on the notion that the functional guidance arises because of aspects of the environment of use (reuse of removable media might be an example of this). If so, then an approach to address this is to provide hints to the PP/ST author about environmental aspects to consider when writing the PP/ST. This would then translate into requirements on the environment, which must then be included in the guidance.

The last approach uses the CEM to provide the guidance. In this approach, the CEM sections that discuss the guidance documentation would provide the functional cases as specific examples of information that must be present.

I-0382: TSF Architectural Protections Are Really Assurances

NUMBER: I-0382
STATUS: Submitted as Request for Interpretation to CCIMB
TYPE: Request for Interpretation

TITLE: TSF Architectural Protections Are Really Assurances

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 10.10 FPT_RVM
CC v2.1 Part 2 Subclause 10.11 FPT_SEP
CC v2.1 Part 2 Subclause 10.12 FPT_SSP
CC v2.1 Part 2 Subclause 10.15 FPT_TRC
CC v2.1 Part 2 Subclause 10.6 FPT_ITT
CC v2.1 Part 2 Subclause J.10 FPT_RVM
CC v2.1 Part 2 Subclause J.11 FPT_SEP
CC v2.1 Part 2 Subclause J.12 FPT_SSP
CC v2.1 Part 2 Subclause J.15 FPT_TRC
CC v2.1 Part 2 Subclause J.6 FPT_ITT
CC v2.1 Part 3
CC v2.1 Part 3 Subclause 10.4 ADV_INT

RELATED TO:
I-0339 Assurance Of RVM Is By Testing And Design Analysis

ISSUE:

Many of the families in the FPT class are really architectural assurances; assurance is gained through design analysis combined with testing through the TOE interface (where possible).

STATEMENT OF INTERPRETATION:

The Common Criteria requires restructuring to properly present those families related to architectural assurances.

PROJECTED IMPACT:

This has a major impact on the structure of the Common Criteria.

SUPPORT:

Background

Many of the families in FPT are "caught in the middle": they are neither clearly functional requirements, nor are they clearly assurance requirements. In versions 1.0 and 2.*x* of the CC, the placement of these families in Part 2 has been problematic, for it is impossible to verify that the requirements of these components are met solely through testing. True verification requires examination of the design and implementation. Additionally, these families, by their nature, have the characteristic of not having a clear functional interface.

On the other hand, the problematic families do not belong in the Part 3 ADV class. The ADV class deals with the decomposition of the design from the high-level functional specification to the implementation. Its goal is to provide confidence that all the functions claimed to be present through the interface are properly implemented. The elements in the Class ADV components are verified solely through design inspection.

The families of particular interest, in CC v2.1 nomenclature, are FPT_RVM and FPT_SEP. These have the characteristic that verification of correctness requires both analysis of design and implementation as well as selective testing.

Investigation for this interpretation also uncovered ADV_INT as a family that is out of place. ADV_INT does not belong in the ADV class, because it is unique in that it places requirements on how the TOE is implemented, not on how the TOE is designed. In this aspect, it is similar to FPT_SEP and FPT_RVM, which also place requirements on implementation.

Potential Solutions

There are four potential solutions to the problems of these components:

1. *Leave things as they are.* This solution has the problem that all the known confusions remain: how are the requirements of the families completely tested through the interface?
2. *Correct the dependencies.* This solution proposed to perform additional dependency analysis to more properly identify the dependencies between functions and assurance. This would allow better identification of the dependencies of EALs upon certain architectural and functional features. However, it fails to show the different approaches to gaining assurance for the indicated components.
3. *Creation of a new Assurance Class.* This solution moves the problematic component into a distinct class for architectural assurances. This distinct class has the common characteristic that assurance is gained through a combination of testing and design analysis.
4. *Creation of a new "Part".* This would create a new part of the Common Criteria for such families that is neither functional nor assurance, but is a hybrid.

Recommendation

The IWG believes that the third approach, creation of a new class, is an acceptable compromise. The first two approaches do not serve to clarify the current confusions, although the notion of showing dependencies of EALs to functions such as RVM and SEP is intriguing. The last approach is too radical. By creating a new class for architectural assurances, it becomes clear that assurance for these families is achieved through a combination of architectural analysis and testing.

Specifically, the IWG proposes restructuring the CC to create in Part 3 a new Architectural Assurances class (NIAP-0382-AAR). This class would contain the current ADV_INT (to be renamed NIAP-0382-AAR_INT) family on Design Internals, as well as the FPT_RVM and FPT_SEP families currently in FPT. Additionally,

if FPT_ITT, FPT_SSP, and FPT_TRC have not been incorporated into FPT_SEP (per I-0380), they should be in NIAP-0382-AAR also. The following families should also be reviewed to see if they are more appropriate for NIAP-0382-AAR: FPT_FLS, FPT_AMT, FPT_RCV.

The structure of each new family would be roughly as follows ("xxx" is SEP, RVM, etc.):

OBJECTIVES

This would be a paraphrase of the current objectives of the family, reworked to put the emphasis on design characteristics as opposed to TOE functional behavior.

COMPONENT LEVELING

Similar to the functional leveling

APPLICATION NOTES

Similar to current application notes

NIAP-0382-AAR_*xxx*.1 TITLE

Dependencies: *As appropriate*

Developer Action Elements:

NIAP-0382-AAR_*xxx*.1.1D. The developer shall provide the design of the TSF.

Content and Presentation of Evidence Elements:

NIAP-0382-AAR_*xxx*.1.1C. The design of the TSF shall demonstrate that *functional elements recast as design requirements*

Evaluator Action Elements

NIAP-0382-AAR_*xxx*.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of elements.

NIAP-0382-AAR_*xxx*.1.2E. The evaluator shall test the architectural characteristics called out by this component that are visible through the TSFI.

Inclusion in Assurance Levels

If the goal is to preserve the current CC EAL structuring, none of these NIAP-0382-AAR components should be included in an EAL, except NIAP-0382-AAR_INT (which was previously included in EALs as ADV_INT). This allows their inclusion to remain at the option of the PP/ST author, as is currently the case for the FPT incarnations.

However, given the importance of NIAP-0382-AAR_SEP to the argument of TSF protection, the IWG strongly supports including the lowest hierarchical component of NIAP-0382-AAR_SEP in all EALs. Additional, given the importance of NIAP-0382-AAR_RVM to ensuring that TSP enforcement functions are invoked and succeed, the IWG strongly supports including the lowest hierarchical component of NIAP-0382-AAR_RVM in all EALs.

Labeling Convention in NIAP Interpretations

The Interpretations Working Group has developed a labeling convention for the identification of new and changed classes, families, components, elements, EALs, and work units. This labeling scheme was developed to make it clear to the national and international users of the CC what is new and changed as a result of NIAP interpretations.

Class/Family/Component/Element/etc. Labeling

A specific labeling convention is used to identify CC or CEM structures (i.e., families, classes, components, elements, work-units) modified or added by NIAP interpretations:

New Items

For new items created by interpretation I-nnnn, the item is identified by NIAP-nnnn-m, where nnnn is the interpretation number, and m is either the new tag (for new classes or families) or (for new components, elements, or work units) a digit to differentiate the item from other new items resulting from the same interpretation. The identification is used in the following fashion:

- **New Class:** If interpretation I-1234 created a new class FEX, the class would be NIAP-1234-FEX.
- **New Family:** If interpretation I-1234 created a new family EXA in existing class FPT, the new family would be FPT_NIAP-1234-EXA
- **New Component:** If interpretation I-1234 created a new component in FPT_SEP, the new component would be FPT_SEP.NIAP-1234-1
- **New Element:** If interpretation I-1234 created a new element in FPT_SEP.1, the new element would be FPT_SEP.1.NIAP-1234-1. Assurance elements would still have "C", "D", or "E" suffixes, as appropriate.
- **New Work Unit:** If interpretation I-1234 created a new work unit for APE_REQ.1, the new work unit would be APE_REQ.1-NIAP-1234-1.

Changed Items

For changes to existing items, a similar NIAP-nnnn notation is used; however, there is no "-m" added. The change is indicated by adding the NIAP tag after that portion of the item name that identifies the changed item, following a dash. For example:

- **Changed Class:** (this applies only when an entire class is replaced): If interpretation I-1234 replaced the entire FMT class, the replacement class would be FMT-NIAP-1234.
- **Changed Family:** If interpretation I-1234 replaced the entire FMT_MOF family, the replacement family would be FMT_MOF-NIAP-1234
- **Changed Component:** If interpretation I-1234 replaced (or relabeled) the FMT_MOF.1 component, the replacement component would be FMT_MOF.1- NIAP-1234.
- **Changed Element:** If interpretation I-1234 replaced FMT_MOF.1.1, the replacement element would be FMT_MOF.1.1-NIAP-1234. Assurance elements would still have "C", "D", or "E" suffixes, as appropriate.
- **Changed Work Unit:** If interpretation I-1234 changed work unit 1:APE_REQ.1-1, the new work unit would be 1:APE_REQ.1-1-NIAP-1234.

Changes to Previously Interpreted Things

When the changed item has a label affected by a prior interpretation, the previous NIAP-nnnn tag is removed. For example, if existing FPT_SEP.1.1-NIAP-1234 is changed by a subsequent interpretation I-5678, the changed tag is FPT_SEP.1.1-NIAP-5678, not FPT_SEP.1.1-NIAP-1234-NIAP-5678.

Affect on Paragraph Numbers

The labeling convention is **not** used for paragraph numbers.

Occasions when the convention is used for Clauses or Subclauses.

Normally, the labeling convention is not used for clauses or subclauses. The convention is used in the following cases:

- New classes, families, or components added to Part 2 or 3. This will result in new subclauses
- New activities or sub-activities added to the CEM.

When the new convention is used

CC Components are relabeled whenever an existing component is modified in a way that would be visible when the component is included in a PP/ST. Components are relabeled in the following situations:

- when an existing element in an existing component is changed.
- when the dependencies of an existing component are changed.
- when the AUDIT section for that component is changed

Relabeling is **not** performed:

- when informative paragraphs in the element (front matter, Annex material) are changed
- when the management sections for a specific component are changed
  Note: Management and Audit sections are actually written at the level of the family; for changes to the audit section, the component is relabeled, yet the family is not.
- solely due to a change in the corresponding CEM workunits
  Note: This may result in a case where the methodology has changed, yet the new methodology used in an evaluation is not readily apparent from the security components identified in the PP/ST. However, the new methodology can be derived from the required list in the ETR of all interpretations that are used during the evaluation.

When a CC component is relabeled, the following text is used (FPT_SEP.1 is used as an example):

- FPT_SEP.1 is relabeled as FPT_SEP.1-NIAP-1234. Unless otherwise noted in these changes, all normative and informative material associated with FPT_SEP.1 is incorporated unchanged into FPT_SEP.1-NIAP-1234, and all references to FPT_SEP.1 in the CC, CEM, or other Common Criteria documentation are changed to refer to FPT_SEP.1-NIAP-1234.

When elements are incorporated without change into a relabeled component, they retain their original numbers.

For example, consider an existing FPT_SEP.1, that has elements FPT_SEP.1.1 and FPT_SEP.1.2. If interpretation I-1234 modifies FPT_SEP.1.2, the relabeled component would be FPT_SEP.1-NIAP-1234, with elements:

- FPT_SEP.1.1
- FPT_SEP.1.2-NIAP-1234

If a subsequent interpretation I-5678 modified FPT_SEP.1-NIAP-1234 to change FPT_SEP.1.1 and add a new element, the relabeled component would be FPT_SEP.1-NIAP-5678, with elements:

- FPT_SEP.1.1-NIAP-5678
- FPT_SEP.1.2-NIAP-1234
- FPT_SEP.1.NIAP-5678-1

Interpretations Index (by Source)

This index pages lists the collected interpretations that have been approved by CCEVS management and the CCEVS RIs sent to the CCIMB, sorted by CC/CEM reference.

- CC v2.1 Part 1 Figure 4.4
  - I-0393: A Completely Evaluated ST Is Not Required When TOE Evaluation Starts (Approved by TTAP/CCEVS Management on 2001-03-15)
- CC v2.1 Part 1 Figure 5.1
  - I-0393: A Completely Evaluated ST Is Not Required When TOE Evaluation Starts (Approved by TTAP/CCEVS Management on 2001-03-15)
- CC v2.1 Part 1 Subclause 2.3
  - I-0395: Security Attributes Include Attributes Of Information And Resources (Approved by TTAP/CCEVS Management on 2001-03-15)
  - I-0411: Guidance Includes AGD_ADM, AGD_USR, ADO, And ALC_FLR (Approved by TTAP/CCEVS Management and Posted on 2000-12-22)
- CC v2.1 Part 1 Subclause 4.2.1
  - I-0378: Meaning Of Compliance Claims (Submitted as Request for Interpretation to CCIMB on 1999-12-17)
- CC v2.1 Part 1 Subclause 4.2.2
  - I-0393: A Completely Evaluated ST Is Not Required When TOE Evaluation Starts (Approved by TTAP/CCEVS Management on 2001-03-15)
- CC v2.1 Part 1 Subclause 4.3
  - I-0378: Meaning Of Compliance Claims (Submitted as Request for Interpretation to CCIMB on 1999-12-17)
- CC v2.1 Part 1 Subclause 4.4.1
  - I-0397: Iteration On Assurance Components/Elements (Approved by TTAP/CCEVS Management on 2001-03-15)
- CC v2.1 Part 1 Subclause 4.4.1.3
  - I-0362: Scope Of Permitted Refinements (Approved by TTAP/CCEVS Management on 2000-03-27)

- CC v2.1 Part 1 Subclause 4.5.3
  - I-0393: A Completely Evaluated ST Is Not Required When TOE Evaluation Starts (Approved by TTAP/CCEVS Management on 2001-03-15)
- CC v2.1 Part 1 Subclause B.2.7
  - I-0364: Application Notes In Protection Profiles Are Informative Only (Approved by TTAP/CCEVS Management on 2000-03-27)
- CC v2.1 Part 1 Subclause C.2.8
  - I-0378: Meaning Of Compliance Claims (Submitted as Request for Interpretation to CCIMB on 1999-12-17)
- CC v2.1 Part 1 Subclause C.2.9
  - I-0355: Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3 (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0418 on 2000-12-05)
  - I-0383: Content Of PP Claims Rationale (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0426 on 2000-12-05)
  - I-0418: Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3 (Approved by TTAP/CCEVS Management and Posted on 2000-12-05)
  - I-0426: Content Of PP Claims Rationale (Approved by TTAP/CCEVS Management and Posted on 2000-12-05)

- CC v2.1 Part 2
  - I-0379: How To Require User/Admin Documentation For Functional Components (Submitted as Request for Interpretation to CCIMB on 2000-02-01)
- CC v2.1 Part 2 Subclause 2.1.4.1
  - I-0394: Iteration Must Cover All Scopes (Approved by TTAP/CCEVS Management and Posted on 2000-12-20)
- CC v2.1 Part 2 Subclause 2.1.4.4
  - I-0362: Scope Of Permitted Refinements (Approved by TTAP/CCEVS Management on 2000-03-27)
- CC v2.1 Part 2 Subclause 3.6 FAU_STG
  - I-0348: Audit Data Loss Prevention Method May Be Site-Selectable (Approved by TTAP/CCEVS Management on 2000-03-27)
  - I-0370: Clarification Of ``Audit Records'' (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0422 on 2000-12-05)
  - I-0371: Some Modifications To The Audit Trail Are Authorized (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0423 on 2000-12-11)

- I-0422: Clarification Of ``Audit Records'' (Approved by TTAP/CCEVS Management and Posted on 2000-12-05)
- I-0423: Some Modifications To The Audit Trail Are Authorized (Approved by TTAP/CCEVS Management and Posted on 2000-12-11)

- CC v2.1 Part 2 Clause 6 FDP
  - I-0363: Attribute Inheritance/Modification Rules Need To Be Included In Policy (Approved by TTAP/CCEVS Management on 2000-03-27)
- CC v2.1 Part 2 Subclause 6.2 FDP_ACF.1
  - I-0353: Association Of Access Control Attributes With Subjects And Objects (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0416 on 2000-12-05)
  - I-0416: Association Of Access Control Attributes With Subjects And Objects (Approved by TTAP/CCEVS Management and Posted on 2000-12-05)
- CC v2.1 Part 2 Subclause 6.6 FDP_IFF
  - I-0354: Association Of Information Flow Attributes W/Subjects And Information (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0417 on 2000-12-11)
- CC v2.1 Part 2 Subclause 6.6 FDP_IFF.1.1
  - I-0417: Association Of Information Flow Attributes W/Subjects And Information (Approved by TTAP/CCEVS Management and Posted on 2000-12-11)
- CC v2.1 Part 2 Subclause 6.6 FDP_IFF.2.1
  - I-0417: Association Of Information Flow Attributes W/Subjects And Information (Approved by TTAP/CCEVS Management and Posted on 2000-12-11)
- CC v2.1 Part 2 Subclause 7.1 FIA_AFL
  - I-0377: Settable Failure Limits Are Permitted (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0425 on 2000-12-05)
  - I-0425: Settable Failure Limits Are Permitted (Approved by TTAP/CCEVS Management and Posted on 2000-12-05)
- CC v2.1 Part 2 Subclause 7.6 FIA_USB
  - I-0352: Rules Governing Binding Should Be Specifiable (Approved by TTAP/CCEVS Management and Posted on 2000-12-20)
- CC v2.1 Part 2 Subclause 7.6 FIA_USB.1
  - I-0351: User Attributes To Be Bound Should Be Specified (Approved by TTAP/CCEVS Management on 2000-03-27)
- CC v2.1 Part 2 Subclause C.6 FAU_STG
  - I-0348: Audit Data Loss Prevention Method May Be Site-Selectable (Approved by TTAP/CCEVS Management on 2000-03-27)

- I-0370: Clarification Of ``Audit Records'' (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0422 on 2000-12-05)
- I-0371: Some Modifications To The Audit Trail Are Authorized (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0423 on 2000-12-11)
- I-0422: Clarification Of ``Audit Records'' (Approved by TTAP/CCEVS Management and Posted on 2000-12-05)
- I-0423: Some Modifications To The Audit Trail Are Authorized (Approved by TTAP/CCEVS Management and Posted on 2000-12-11)

- CC v2.1 Part 2 Annex F FDP
  - I-0363: Attribute Inheritance/Modification Rules Need To Be Included In Policy (Approved by TTAP/CCEVS Management on 2000-03-27)
- CC v2.1 Part 2 Subclause F.2 FDP_ACF.1
  - I-0353: Association Of Access Control Attributes With Subjects And Objects (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0416 on 2000-12-05)
  - I-0416: Association Of Access Control Attributes With Subjects And Objects (Approved by TTAP/CCEVS Management and Posted on 2000-12-05)
- CC v2.1 Part 2 Subclause F.6 FDP_IFF
  - I-0354: Association Of Information Flow Attributes W/Subjects And Information (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0417 on 2000-12-11)
  - I-0417: Association Of Information Flow Attributes W/Subjects And Information (Approved by TTAP/CCEVS Management and Posted on 2000-12-11)
- CC v2.1 Part 2 Subclause G.1 FIA_AFL
  - I-0377: Settable Failure Limits Are Permitted (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0425 on 2000-12-05)
  - I-0425: Settable Failure Limits Are Permitted (Approved by TTAP/CCEVS Management and Posted on 2000-12-05)
- CC v2.1 Part 2 Subclause G.4 FIA_UAU
  - I-0375: Elements Requiring Authentication Mechanism (Approved by TTAP/CCEVS Management on 2001-03-15)
- CC v2.1 Part 2 Subclause G.6 FIA_USB
  - I-0352: Rules Governing Binding Should Be Specifiable (Approved by TTAP/CCEVS Management and Posted on 2000-12-20)
- CC v2.1 Part 2 Subclause G.6 FIA_USB.1
  - I-0351: User Attributes To Be Bound Should Be Specified (Approved by TTAP/CCEVS Management on 2000-03-27)

- CC v2.1 Part 2 Clause J FPT_SEP
  - I-0424: FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical (Approved by TTAP/CCEVS Management and Posted on 2000-12-05)
- CC v2.1 Part 2 Subclause J.6 FPT_ITT
  - I-0382: TSF Architectural Protections Are Really Assurances (Submitted as Request for Interpretation to CCIMB on 2001-03-01)
- CC v2.1 Part 2 Subclause J.8 FPT_RCV
  - I-0389: Recovery To A Known State (Approved by TTAP/CCEVS Management on 2001-03-15)
  - I-0406: Automated Or Manual Recovery Is Acceptable (Approved by TTAP/CCEVS Management on 2001-03-15)
- CC v2.1 Part 2 Subclause J.10 FPT_RVM
  - I-0339: Assurance Of RVM Is By Testing And Design Analysis (Approved by TTAP/CCEVS Management on 2000-03-27)
  - I-0382: TSF Architectural Protections Are Really Assurances (Submitted as Request for Interpretation to CCIMB on 2001-03-01)
- CC v2.1 Part 2 Subclause J.11 FPT_SEP
  - I-0373: FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0424 on 2000-12-05)
  - I-0382: TSF Architectural Protections Are Really Assurances (Submitted as Request for Interpretation to CCIMB on 2001-03-01)
  - I-0424: FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical (Approved by TTAP/CCEVS Management and Posted on 2000-12-05)
- CC v2.1 Part 2 Subclause J.12 FPT_SSP
  - I-0382: TSF Architectural Protections Are Really Assurances (Submitted as Request for Interpretation to CCIMB on 2001-03-01)
- CC v2.1 Part 2 Subclause J.15 FPT_TRC
  - I-0382: TSF Architectural Protections Are Really Assurances (Submitted as Request for Interpretation to CCIMB on 2001-03-01)
- CC v2.1 Part 2 Clause 10 FPT_SEP
  - I-0424: FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical (Approved by TTAP/CCEVS Management and Posted on 2000-12-05)
- CC v2.1 Part 2 Subclause 10.6 FPT_ITT
  - I-0382: TSF Architectural Protections Are Really Assurances (Submitted as Request for Interpretation to CCIMB on 2001-03-01)

- CC v2.1 Part 2 Subclause 10.8 FPT_RCV
  - I-0389: Recovery To A Known State (Approved by TTAP/CCEVS Management on 2001-03-15)
  - I-0406: Automated Or Manual Recovery Is Acceptable (Approved by TTAP/CCEVS Management on 2001-03-15)
- CC v2.1 Part 2 Subclause 10.10 FPT_RVM
  - I-0339: Assurance Of RVM Is By Testing And Design Analysis (Approved by TTAP/CCEVS Management on 2000-03-27)
  - I-0382: TSF Architectural Protections Are Really Assurances (Submitted as Request for Interpretation to CCIMB on 2001-03-01)
- CC v2.1 Part 2 Subclause 10.11 FPT_SEP
  - I-0373: FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0424 on 2000-12-05)
  - I-0382: TSF Architectural Protections Are Really Assurances (Submitted as Request for Interpretation to CCIMB on 2001-03-01)
  - I-0424: FPT_SEP.2 And FPT_SEP.3 Are Not Hierarchical (Approved by TTAP/CCEVS Management and Posted on 2000-12-05)
- CC v2.1 Part 2 Subclause 10.12 FPT_SSP
  - I-0382: TSF Architectural Protections Are Really Assurances (Submitted as Request for Interpretation to CCIMB on 2001-03-01)
- CC v2.1 Part 2 Subclause 10.15 FPT_TRC
  - I-0382: TSF Architectural Protections Are Really Assurances (Submitted as Request for Interpretation to CCIMB on 2001-03-01)

- CC v2.1 Part 3
  - I-0382: TSF Architectural Protections Are Really Assurances (Submitted as Request for Interpretation to CCIMB on 2001-03-01)
- CC v2.1 Part 3 Subclause 2.1.3.5
  - I-0397: Iteration On Assurance Components/Elements (Approved by TTAP/CCEVS Management on 2001-03-15)
- CC v2.1 Part 3 Subclause 2.1.4
  - I-0379: How To Require User/Admin Documentation For Functional Components (Submitted as Request for Interpretation to CCIMB on 2000-02-01)
  - I-0397: Iteration On Assurance Components/Elements (Approved by TTAP/CCEVS Management on 2001-03-15)

- CC v2.1 Part 3 Subclause 3.1
  - I-0393: A Completely Evaluated ST Is Not Required When TOE Evaluation Starts (Approved by TTAP/CCEVS Management on 2001-03-15)
- CC v2.1 Part 3 Clause 4 APE
  - I-0364: Application Notes In Protection Profiles Are Informative Only (Approved by TTAP/CCEVS Management on 2000-03-27)
- CC v2.1 Part 3 Subclause 4.5 APE_REQ
  - I-0385: Identification Of Standards (Approved by TTAP/CCEVS Management on 2000-03-27)
- CC v2.1 Part 3 Subclause 5.5 ASE_PPC
  - I-0378: Meaning Of Compliance Claims (Submitted as Request for Interpretation to CCIMB on 1999-12-17)
  - I-0383: Content Of PP Claims Rationale (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0426 on 2000-12-05)
  - I-0426: Content Of PP Claims Rationale (Approved by TTAP/CCEVS Management and Posted on 2000-12-05)
- CC v2.1 Part 3 Subclause 5.6 ASE_REQ
  - I-0385: Identification Of Standards (Approved by TTAP/CCEVS Management on 2000-03-27)
- CC v2.1 Part 3 Subclause 5.8 ASE_TSS
  - I-0355: Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3 (Approved by TTAP/CCEVS Management on 2000-03-27; superseded by 0418 on 2000-12-05)
  - I-0418: Evaluation Of The TOE Summary Specification: Part 1 Vs Part 3 (Approved by TTAP/CCEVS Management and Posted on 2000-12-05)
- CC v2.1 Part 3 Subclause 8.2 ACM_CAP.2
  - I-0338: Configuration Items In The Absence Of Explicit Scope (Approved by TTAP/CCEVS Management on 2000-03-27)
- CC v2.1 Part 3 Subclause 10.4 ADV_INT
  - I-0382: TSF Architectural Protections Are Really Assurances (Submitted as Request for Interpretation to CCIMB on 2001-03-01)
- CC v2.1 Part 3 Clause 11 AGD
  - I-0379: How To Require User/Admin Documentation For Functional Components (Submitted as Request for Interpretation to CCIMB on 2000-02-01)
  - I-0411: Guidance Includes AGD_ADM, AGD_USR, ADO, And ALC_FLR (Approved by TTAP/CCEVS Management and Posted on 2000-12-22)

- CEM v1.0 Part 2 Subclause 3.4.5 APE_REQ
  - I-0405: American English Is An Acceptable Refinement (Approved by TTAP/CCEVS Management and Posted on 2000-12-20)
- CEM v1.0 Part 2 Subclause 3.4.5 APE_REQ.1
  - I-0394: Iteration Must Cover All Scopes (Approved by TTAP/CCEVS Management and Posted on 2000-12-20)
- CEM v1.0 Part 2 Subclause 4.4.6 ASE_REQ
  - I-0362: Scope Of Permitted Refinements (Approved by TTAP/CCEVS Management on 2000-03-27)
  - I-0405: American English Is An Acceptable Refinement (Approved by TTAP/CCEVS Management and Posted on 2000-12-20)
- CEM v1.0 Part 2 Subclause 4.4.6 ASE_REQ.1
  - I-0394: Iteration Must Cover All Scopes (Approved by TTAP/CCEVS Management and Posted on 2000-12-20)
